ADSL Modem

HM210dp/di

User Guide

ERICSSON

ADSL Modem

HM210dp/di

User Guide

.

Copyright

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Ericsson shall have no liability for any error or damages of any kind resulting from the use of this document.

Abstract

This User guide describes how to install and set up the Ericsson ADSL Modem HM210dp/di in a Windows environment, and how to customize its configuration to get the most out of the product.

Trademark List

Windows	Windows is a registered trademark of Microsoft Corporation

Enclosure List

Contents

1 Introduction

Congratulations on becoming the owner of an Ericsson ADSL Modem HM210dp/di. Your LAN (Local Area Network) will now be able to access the Internet using your high-speed ADSL connection.

1.1 About this User Guide

This User Guide describes how to install and setup your HM210dp/di in a Windows environment, and how to customize its configuration to get the most out of your new product.

The **Glossary** includes abbreviations and explanations to technical terms used in this guide.

1.2 About the ADSL Modem HM210d

The ADSL Modem HM210 comes in two versions: HM210dp and HM210di. Both products offer the same features, but they rely on different types of telephone line in order to provide the ADSL service. **HM210dp** offers ADSL service over POTS (Plain Old Telephone System) lines, while **HM210di** uses ISDN (Integrated Services Digital Network) lines to provide the ADSL service.

1.2.1 Features

The main features of the HM210dp/di are listed below:

- Internal ADSL modem for high-speed Internet access.
- 10/100Base-T Ethernet router to provide Internet connectivity to all computers on your LAN.
- Network Address Translation (NAT), Firewall and IP filtering functions to provide security for your LAN.
- Network configuration through DHCP Server and DHCP Relay.
- Services including IP route and DNS configuration, RIP, and IP and DSL performance monitoring.
- Configuration Manager program you access via a web browser.

2 Hardware Description and Installation

This chapter describes the product and provides instructions about how to install the HM210dp/di in a PC/Windows environment.

2.1 Before You Start

2.1.1 Package Contents

Check the contents of the package against the shipping contents checklist below. If any of the items is missing, please contact the ADSL modem provider.

- ❑ The ADSL Modem HM210dp/di
- ❑ A Power Supply Adapter with connecting cable
- ❑ ADSL Line Cable (RJ-11)
- ❑ Ethernet Cable (RJ-45)
- ❑ USB Cable
- ❑ Quick Installation Guide
- ❑ Documentation CD (including Acrobat Reader and this User Guide)

Your HM210dp/di package may also include other materials provided by your ADSL operator.

2.1.2 Subscription for ADSL Service

To use the ADSL Modem HM210dp/di, you will require an ADSL service subscription from your broadband service provider.

2.1.3 System Requirements

In order to use your HM210dp/di you must have the following:

- ❑ One or more computers each containing an Ethernet 10/100Base-T network interface card (NIC).

- An Ethernet hub/switch if you are connecting the device to more than one computer.
- For system configuration using the built-in Configuration Manager program you need a web browser such as Internet Explorer v5.0 or later, or Netscape v5.0 or later.

2.2 Physical Appearance

2.2.1 Front Panel and LED Indicators

The front panel of the HM210dp/di contains five control lamps (LEDs) that indicate the status of the modem. A general description of each LED is provided in the table below (from left to right):

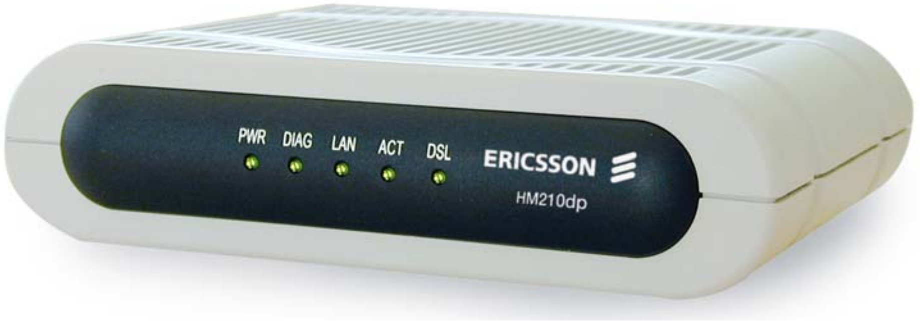


Figure 1 - Front Panel of HM210dp

Label	Status/Description
PWR	**On**: Unit is powered on. **Off**: Unit is powered off.
DIAG	**Flashes** on/off at boot-up to indicate that the device software is operational. Turns off after 10-15 seconds.
LAN	**On**: Ethernet link established and active. **Off**: No Ethernet link detected.
ACT	**Flashes** when ADSL data activity occurs. May appear solid when data traffic is heavy.
DSL	**On**: ADSL link established and active. **Off**: No ADSL link detected.

Table 1 - Description of LEDs

2.2.2 Back Panel and Connectors

The following figure illustrates the back panel of your HM210dp/di:

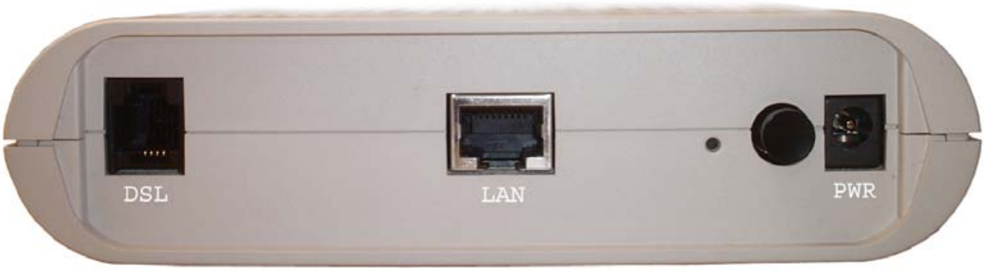


Figure 2 - Back Panel of the HM210dp/di

Description of connectors and buttons:

- **DSL** – The DSL port is used for connecting the HM210dp/di to the ADSL service port (splitter/filter or phone outlet) using the supplied ADSL line cable (RJ11 – RJ11).
- **LAN** – The LAN port (Ethernet 10/100 BaseT) connect the HM210dp/di to your PC's Ethernet port, or to the uplink port on your LAN's hub, using the supplied Ethernet cable (RJ45 – RJ45).
- **RESET button** (tiny hole) – Used to reset and restore the HM210dp/di to default settings.
  Push a paper clicp into the hole and hold for three seconds before releasing. Then wait for the device to finish boot up.
- **Power button** – Used to switch the HM210dp/di ON and OFF.
- **PWR** – Power socket for connecting the HM210dp/di to a power outlet by using the supplied power adapter.

2.3 Choosing a Place for the Router

The HM210dp/di should be placed on a flat surface. Be sure to choose a location that enables you to see the LEDs, is close to a power outlet, ADSL outlet, and the PC.

NOTE! Proper ventilation is necessary to prevent the product from over-heating. Do not block or cover the slots and openings on the device, which are intended for ventilation and proper operation.

2.4 Connecting the Hardware

Follow the procedures below to connect related devices.

NOTE! Before you begin, turn the power off for all devices. These include your computer(s), your LAN hub/switch (if applicable), and the HM210dp/di.

1. **Connect to the ADSL Line**
   Connect one end of the provided **ADSL Line cable** to the port labeled **DSL** on the back panel of the HM210dp/di. Connect the other end to your ADSL service port (splitter/filter or phone outlet).

2. **Connect to a PC or hub/switch:**

   - to a single PC
   Attach one end of the provided **Ethernet cable** (straight-through) to the port labeled **LAN** on the HM210dp/di. Connect the other end to your PC’s Ethernet port.

   - to a hub/switch
   Attach one end of a “cross-over” Ethernet cable to a hub/switch and the other end to the **LAN** port on the HM210dp/di.

   - to a hub/switch’s uplink port
   Use a “straight-through” Ethernet cable to connect to the uplink port and the other end to the **LAN** port on the HM210dp/di.

3. **Connect the Power Supply**
   Connect the provided **Power cable** from the Power Supply Adapter to the **PWR** socket on the HM210dp/di. Plug the power supply adapter into a power source (wall outlet or power strip).

4. **Turn on the HM210dp/di and power up your systems**
   Press the **Power** button on the back panel of the HM210dp/di to turn on the device.

   Turn on and boot up your computer(s) and any LAN devices such as hubs or switches.

3 Local PC Configuration

By default, the HM210dp/di acts as a DHCP server that automatically assigns all required Internet settings to your PCs, i.e. the DHCP clients. The predefined IP address and DHCP range is as below:

LAN Port IP Address	**192.168.1.1**
Subnet Mask	**255.255.255.0**
DHCP Range	**192.168.1.3 – 192.168.1.34**

The following instructions assume that your PC meets the following prerequisites:

1. Already is connected to the LAN port on the HM210dp/di through its network interface card (NIC).

2. Has the appropriate Ethernet adapter software installed.

3. Has the TCP/IP protocol installed. If not, refer to Microsoft documentation to install the TCP/IP protocol.

You need only to configure the PCs to accept the information when it is assigned. Follow the instructions that correspond to the operating system installed on each PC.

3.1 Configuring PCs as DHCP Clients

If you have not been provided any IP settings from your ISP/service provider, you should use DHCP that is the most common used method.

3.1.1 In Windows 95, 98/98SE and Me:

1. From the **Start** menu select **Settings > Control Panel** and double-click on the **Network** icon.

2. Click the **Configuration** tab and select **TCP/IP** for the network adapter that is connected to your HM210dp/di. Click the **Properties** button.

3. Select the **IP Address** tab and make sure that “Obtain an IP address automatically” is selected. If not, select it and click **OK**.

4. Click **OK** in the “Network” dialog box and close the Control Panel.

5. Some configuration files may be copied to your hard disk and if a “Settings Changes” message asks you to restart your PC, you should answer **Yes**.

3.1.2 In Windows 2000:

1. From the **Start** menu select **Settings > Control Panel** and double-click on the **Network and Dial-up Connections** icon.

2. Double-click on the Local Area Connection icon for the HM310dp. Be sure to choose the correct one if you have several dial-up icons.

3. Click the **Properties** button.

4. Select the **Internet Protocol (TCP/IP)** and click the **Properties** button.

5. Make sure that “Obtain an IP address automatically” is selected. If not, select it and click **OK**.

6. Click **OK** in the “Local Area Connection Properties” dialog box and click **Close** in the “Local Area Connection Status” dialog box.

7. Close the “Network and Internet Connections” window.

3.1.3 In Windows XP:

1. From the **Start** menu select **Control Panel** and double-click on **Network Connections** (Classic View) or double-click on the link **Network and Internet connections** followed by **Network Connections** (Category View).

2. Double-click on the Local Area Connection icon for the HM310dp. Be sure to choose the correct one if you have several dial-up icons.

3. Click the **Properties** button.

4. Select the **Internet Protocol (TCP/IP)** and click the **Properties** button.

5. Make sure that “Obtain an IP address automatically” is selected. If not, select it and click **OK**.

6. Click **Close** in the “Local Area Connection Properties” and “Local Area Connection Status” dialog boxes.

7. Close the “Network and Internet Connections” window.

3.2 Assigning Static IP Addresses to your PCs

In some cases, you may want to assign static IP information to your PCs directly if:

- ❑ In **bridged** mode, you have completed the initial configuration and you need to use the IP address and default gateway given by your ISP.
- ❑ You have obtained one or more public IP addresses that you want to always associate with specific computers (for example, if you are using a computer as a public web server).
- ❑ You maintain different subnets on your LAN.

Before you begin, contact your ISP/service provider if you do not already have the following information:

- ❑ IP address and subnet mask
- ❑ Default Gateway IP address
- ❑ DNS Server IP address

Follow the instructions that correspond to the operating system installed on each PC:

3.2.1 In Windows 95, 98/98SE and Me:

1. From the **Start** menu select **Settings > Control Panel** and double-click on the **Network** icon.
2. Click the **Configuration** tab and select **TCP/IP** for the network adapter (Ethernet or USB) that is connected to your HM310dp. Click the **Properties** button.
3. Select the **IP Address** tab.
4. Select “Specify an IP address” and enter the IP settings provided by your ISP/service provider. Click **OK**.
5. Click **OK** in the “Network” dialog box and close the Control Panel.
6. Some configuration files may be copied to your hard disk and if a “Settings Changes” message asks you to restart your PC, you should answer **Yes**.

3.2.2 In Windows 2000:

1. From the **Start** menu select **Settings > Control Panel** and double-click on the **Network and Dial-up Connections** icon.

2. Double-click on the Local Area Connection icon for the HM310dp. Be sure to choose the correct one if you have several dial-up icons.

3. Click the **Properties** button.

4. Select the **Internet Protocol (TCP/IP)** and click the **Properties** button.

5. Select “Specify an IP address” and enter the IP settings provided by your ISP/service provider. Click **OK**.

6. Click **OK** in the “Local Area Connection Properties” dialog box and click **Close** in the “Local Area Connection Status” dialog box.

7. Close the “Network and Internet Connections” window.

3.2.3 In Windows XP:

1. From the **Start** menu select **Control Panel** and double-click on **Network Connections** (Classic View) or double-click on the link **Network and Internet connections** followed by **Network Connections** (Category View).

2. Double-click on the Local Area Connection icon for the HM310dp. Be sure to choose the correct one if you have several dial-up icons.

3. Click the **Properties** button.

4. Select the **Internet Protocol (TCP/IP)** and click the **Properties** button.

5. Select “Use the following IP address” and enter the IP settings provided by your ISP/service provider. Click **OK**.

6. Click **Close** in the “Local Area Connection Properties” and “Local Area Connection Status” dialog boxes.

7. Close the “Network and Internet Connections” window.

4 Getting Started with the Configuration Manager

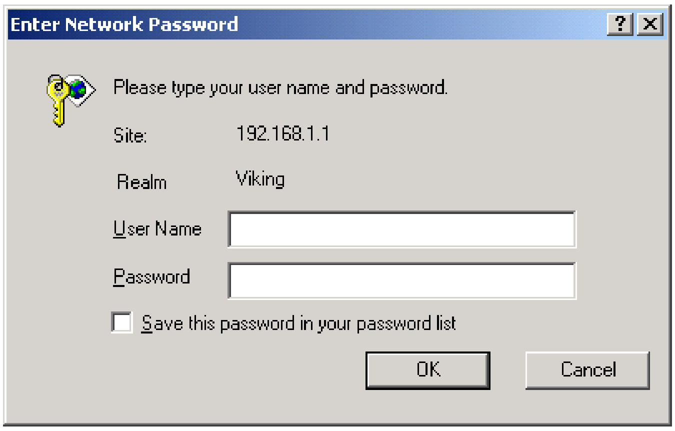
Your HM210dp/di includes a web-based Configuration Manager, which enables you to configure the device settings to meet the needs of your network.

4.1 Accessing the Configuration Manager

You can access the Configuration Manager from any computer connected to the HM210dp/di. Follow the instructions below:

1. At any PC connected to the HM210dp/di, open a web browser, type the following URL in the address (or location) box, and press <Enter>:
   http://192.168.1.1

2. When the Login screen appears, enter your User Name and Password and then click **OK:**



Enter Network Password

Please type your user name and password.

Site: 192.168.1.1

Realm Viking

User Name

Password

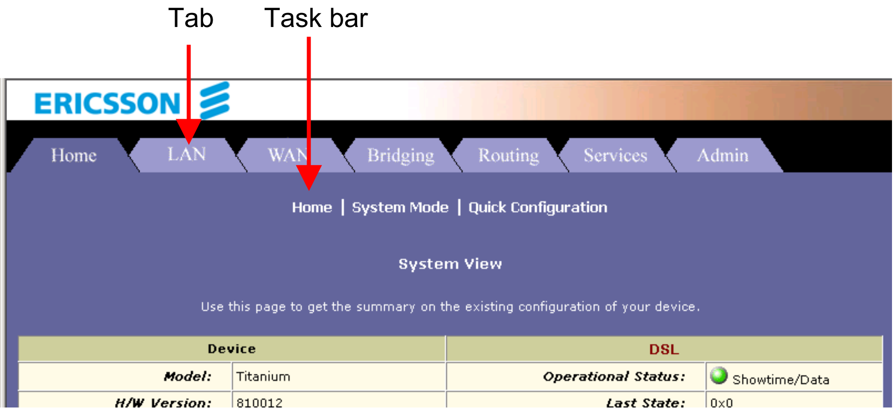
□ Save this password in your password list

The first time you launch the Configuration Manager, use these default values:
Default User Name: **root** Default Password: **root**

3. After a successful login, the home page - **System View** - of the Configuration Manager appears. See section 4.3 for further information.

4.2 Functional Layout

The Configuration Manager tasks are grouped into categories, which you can access by clicking the tabs at the top of each page. Each tab displays the available tasks in a horizontal menu at the top of the page. You can click on these menu items to display the specific configuration options.



System View

Use this page to get the summary on the existing configuration of your device.

Device		DSL	
Model:	Titanium	Operational Status:	Showtime/Data
H/W Version:	810012	Last State:	0x0

A separate page displays for each task in the task bar. The left-most task displays by default when you click on a new tab. The same task may appear in more than one tab, when appropriate. For example, the **LAN Config** task displays in both the **LAN** tab and the **Routing** tab.

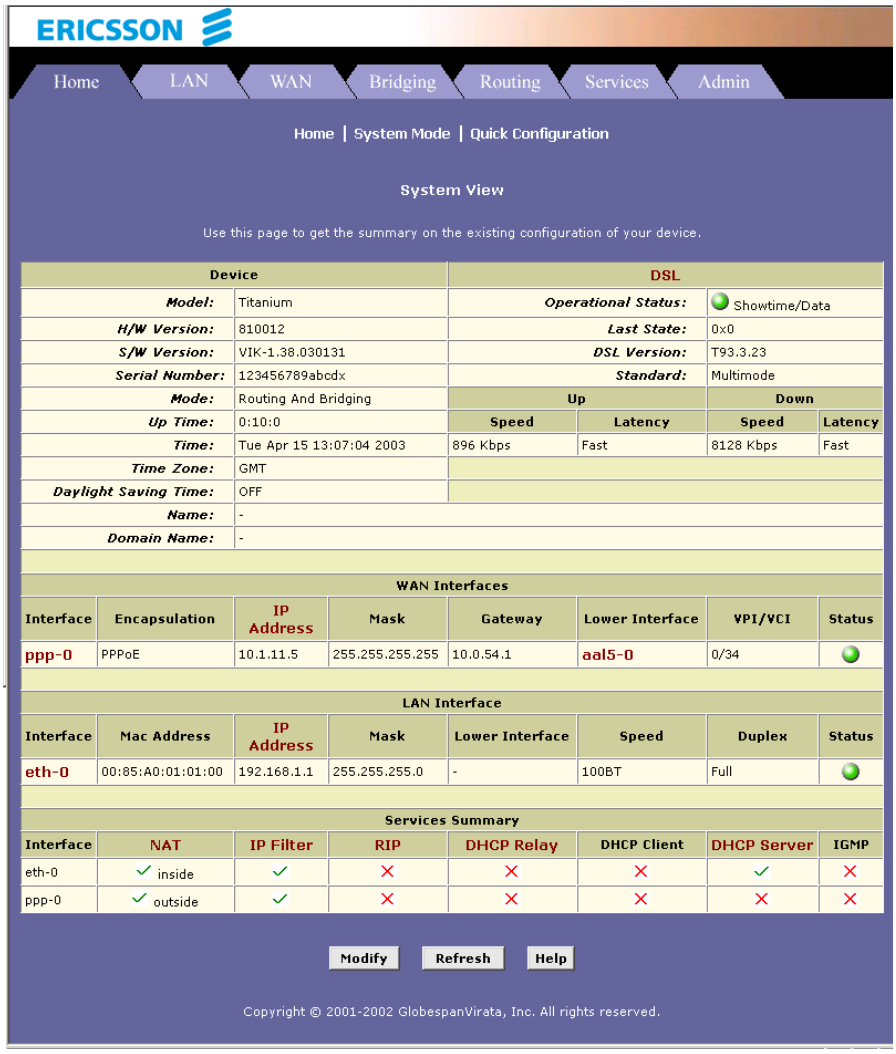
4.2.1 Commonly Used Buttons and Icons

The table below describes buttons and icons commonly used in the Configuration Manager.

Button / Symbol	Description
Submit	Stores in *temporary* system memory any changes you have made on the current page. See section 4.4 “Committing Changes and Rebooting” for instructions on how to store changes permanently.
Refresh	Redisplays the current page with updated statistics or settings.
Clear	When accumulated statistics are displaying, this button resets the statistics to their initial value.
Help	Launches the online help for the current topic in a separate browser window. Help is available from any main topic page.
🗑	Delete an entry.
✎	Modify an entry.
🔍	View details for an entry.

4.3 The Home Page and System View Table

The Home page - **System View** – displays when you first access the Configuration Manager. This page is one of two options available in the Home tab (the other is the Quick Configuration page, as described in section 4.5).



System View

Use this page to get the summary on the existing configuration of your device.

Device		DSL			
Model:	Titanium	*Operational Status:*		● Showtime/Data	
H/W Version:	810012	*Last State:*		0x0	
S/W Version:	VIK-1.38.030131	*DSL Version:*		T93.3.23	
Serial Number:	123456789abcdx	*Standard:*		Multimode	
Mode:	Routing And Bridging	Up		Down	
Up Time:	0:10:0	Speed	Latency	Speed	Latency
Time:	Tue Apr 15 13:07:04 2003	896 Kbps	Fast	8128 Kbps	Fast
Time Zone:	GMT				
Daylight Saving Time:	OFF				
Name:	-				
Domain Name:	-				

WAN Interfaces

Interface	Encapsulation	IP Address	Mask	Gateway	Lower Interface	VPI/VCI	Status
ppp-0	PPPoE	10.1.11.5	255.255.255.255	10.0.54.1	aal5-0	0/34	●

LAN Interface

Interface	Mac Address	IP Address	Mask	Lower Interface	Speed	Duplex	Status
eth-0	00:85:A0:01:01:00	192.168.1.1	255.255.255.0	-	100BT	Full	●

Services Summary

Interface	NAT	IP Filter	RIP	DHCP Relay	DHCP Client	DHCP Server	IGMP
eth-0	✓ inside	✓	✗	✗	✗	✓	✗
ppp-0	✓ outside	✓	✗	✗	✗	✗	✗

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

The **System View** table provides a snapshot of your system configuration. Note that some of the settings are links to the software pages that enable you to configure those settings. The following table describes each section of the System View table:

Table Heading	Description
Device	Displays basic information about the HM210dp/di hardware and software versions, the system uptime (since the last reboot), and the preconfigured operating mode.
DSL	Displays the operational status, version, and performance statistics for the DSL line. You can click on DSL in the table heading or display the WAN tab to view additional DSL settings, which are described in chapter x.
WAN Interfaces	Displays the software name(s) and various settings for the device interface(s) that communicates with your ISP via DSL. Although you only have one physical DSL port, multiple software-defined interfaces can be configured to use it. For each interface, a “Lower Interface” name, such as *aal5-0*, should display. You can click on the lower interface name to view or change the ATM VC settings that this interface uses.
LAN Interfaces	Displays the software names and various settings for the device interfaces that communicate directly with your network. This typically includes an Ethernet interface named *eth-0*.
Services Summary	Displays the status of various services that the HM210dp/di performs to help you manage your network. A green ball indicates the service is active and a red X indicates that it is inactive: **NAT** – Translating private IP addresses to your public IP address. **IP Filter** – Setting up filtering rules that accept or deny incoming or outgoing data. **RIP** – Enabling router-to-router communication. **DHCP Relay** – Enabling dynamic assignment of IP information from your ISP to your computers. **DHCP Client** – Enabling dynamic assignment of IP information from your ISP or another computer on your network to the device’s LAN port. **DHCP Server** – Enabling dynamic assignment of IP information from the device’s built-in DHCP server to your LAN computers. **IGMP** – Enabling message forwarding from external sources such as your ISP, based on Internet Group Management Protocol (not configurable).

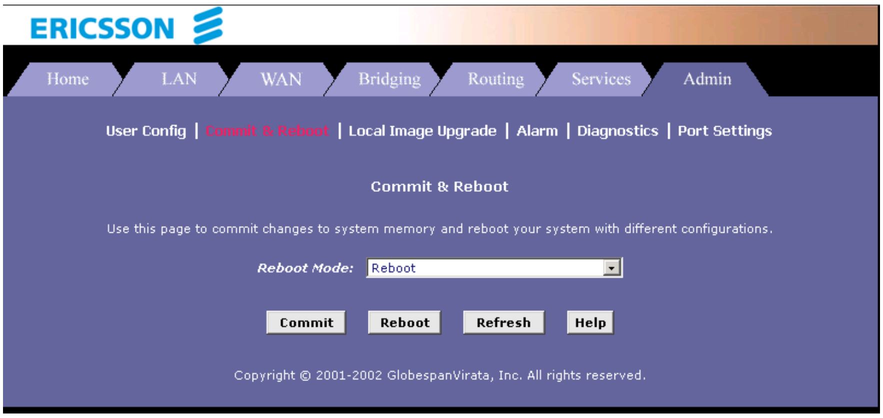
4.4 Commiting Changes and Rebooting

Whenever you change system settings, the changes are initially placed in a temporary storage (called random access memory or RAM). Your changes are made effective when you submit them, but will be lost if the device is reset or turned off.

NOTE! ***Submitting*** changes activates them immediately, but saves them only until the device is reset or powered down. ***Committing*** changes saves them permanently.

Follow these steps to commit changes to permanent storage:

1. Select **Admin > Commit & Reboot**. The **Commit & Reboot** page appears:


ERICSSON
Home
LAN
WAN
Bridging
Routing
Services
Admin
User Config | Commit & Reboot | Local Image Upgrade | Alarm | Diagnostics | Port Settings
Commit
Reboot
Refresh
Help

Commit & Reboot

Use this page to commit changes to system memory and reboot your system with different configurations.

Reboot Mode: Reboot

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

2. Click the **Commit** button. (Disregard the selection in the *Reboot Mode:* dropdown list, it does not affect the commit process). The changes are saved to permanent storage.

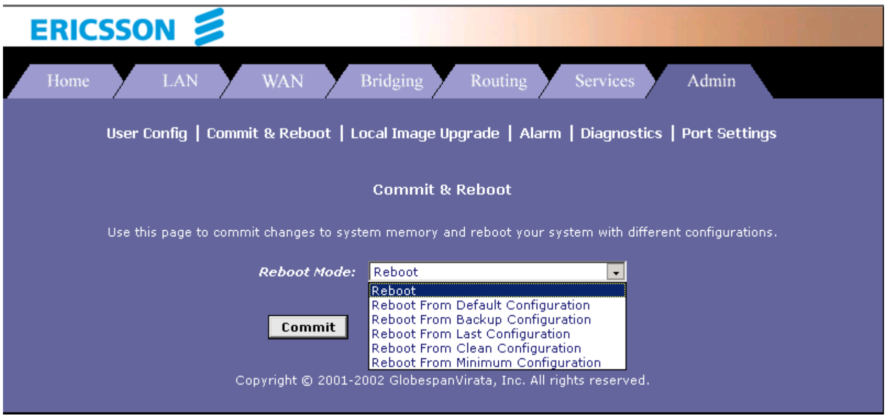
   The previous settings are copied to backup storage so that they can be recalled if your new settings do not work properly (see the rebooting instructions in section 4.4.1).

NOTE! If you change the LAN IP address information, you MUST commit the changes and then reboot the system to activate them. All other changes are activated when you commit them (no reboot is needed).

4.4.1 Rebooting the HM210dp/di using Options

If, after rebooting the device, you find that it does not operate properly with the new configuration, you can reboot using options that reactivate a previous configuration or the factory default configuration.

1. Select **Admin > Commit & Reboot**. The **Commit & Reboot** page appears:


ERICSSON
Home
LAN
WAN
Bridging
Routing
Services
Admin
User Config | Commit & Reboot | Local Image Upgrade | Alarm | Diagnostics | Port Settings
Commit

Commit & Reboot

Use this page to commit changes to system memory and reboot your system with different configurations.

Reboot Mode: Reboot

- Reboot
- Reboot From Default Configuration
- Reboot From Backup Configuration
- Reboot From Last Configuration
- Reboot From Clean Configuration
- Reboot From Minimum Configuration

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

2. In the *Reboot Mode:* dropdown list you can select from the following options before clicking the **Reboot** button.

Setting	Description
Reboot	Reboots the device to activate your new settings (if any).
Reboot from Default Configuration	Reboots the device to default settings provided by your ISP or the manufacturer. Choosing this option erases any custom settings.
Reboot from Backup Configuration	Reboots the device using settings stored in backup memory. These are the settings that were in effect before you committed new settings in the current session.
Reboot from Last Configuration	Reboots the device using the current settings in permanent memory, including any changes you just committed.
Reboot from Clean Configuration	

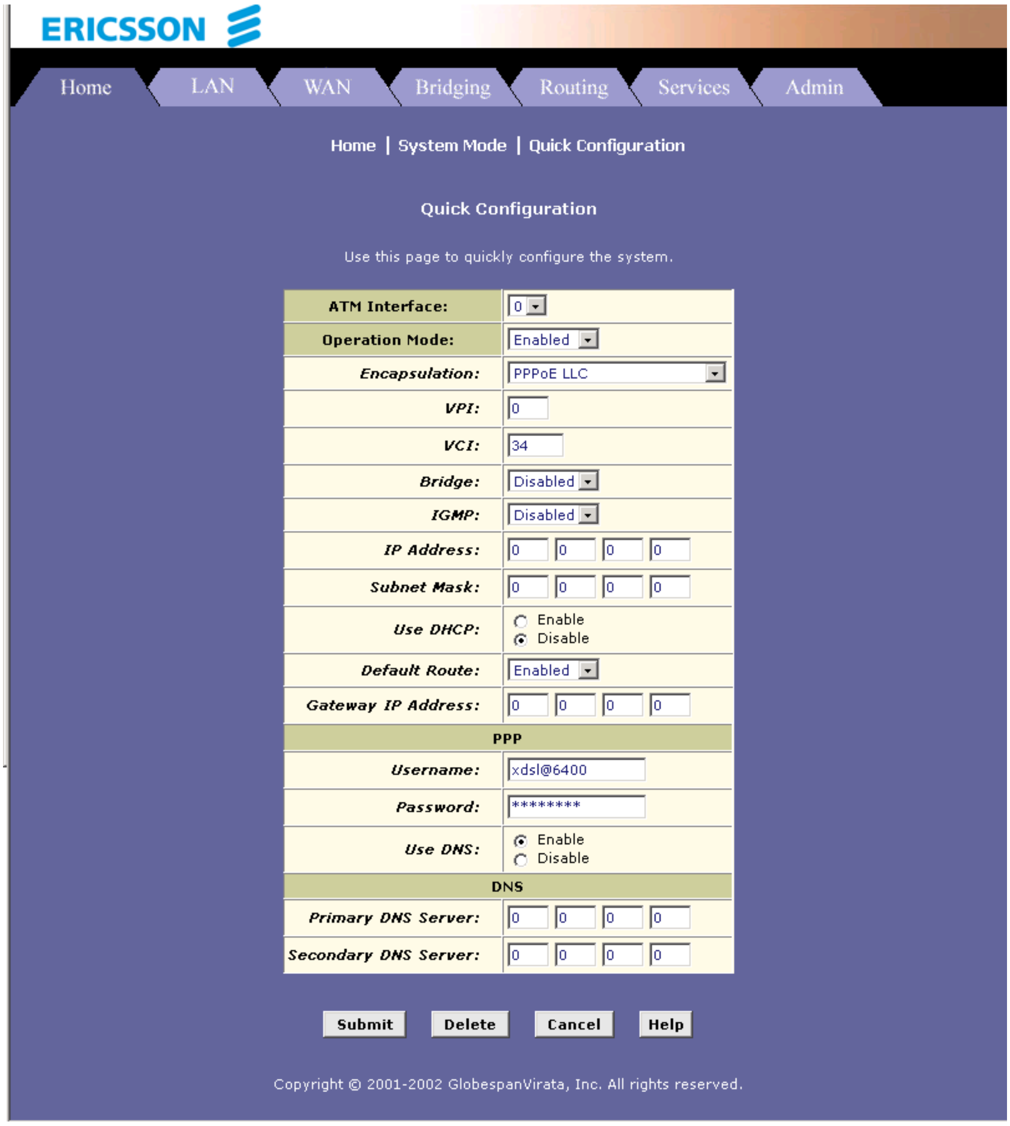
Reboot from Minimum Configuration	

NOTE! Do not reboot the device using the Reset button on the back panel of the HM210dp/di to activate new changes. This button resets the device settings to the manufacturer’s default values. Any custom settings will be lost.

4.5 Quick Configuration

The **Quick Configuration** page allows you to quickly configure your HM210dp/di for Internet connection. Your ISP should provide you with necessary information to complete the quick setup.

To quickly configure the system, go to **Home > Quick Configuration**. The **Quick Configuration** page appears:



Quick Configuration

Use this page to quickly configure the system.

ATM Interface:	0
Operation Mode:	Enabled
Encapsulation:	PPPoE LLC
VPI:	0
VCI:	34
Bridge:	Disabled
IGMP:	Disabled
IP Address:	0 0 0 0
Subnet Mask:	0 0 0 0
Use DHCP:	○ Enable ● Disable
Default Route:	Enabled
Gateway IP Address:	0 0 0 0
PPP	
Username:	xdsl@6400
Password:	********
Use DNS:	● Enable ○ Disable
DNS	
Primary DNS Server:	0 0 0 0
Secondary DNS Server:	0 0 0 0

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Enter the provided fields as below:

Field	Description
ATM Interface:	Select the ATM interface you want to use (usually atm-0) for this connection.
Operation Mode:	**Enabled/Disabled**. If set to **Disabled**, the device cannot provide Internet connectivity for your network.
Encapsulation:	Select the connection type your ISP uses to communicate with your HM210dp/di.
VPI and VCI:	Enter the VPI/VCI values given by your ISP.
Bridge:	This setting enables or disables bridging between the HM210dp/di and your ISP. Your ISP may also refer to this using RFC 1483" or "Ethernet over ATM".
IGMP:	This setting enables or disables the Internet Group Management Protocol. Contact your ISP whether to enable this setting.
IP Address: and Subnet Mask:	If your ISP has assigned a public IP address to your LAN, enter the IP address and associated subnet mask in the boxes provided.
Use DHCP:	Select **Enable** if you want the HM210dp/di to act as a DHCP server for your LAN.
Default Route:	When enabled, the IP address specified above will be used as the default route for your LAN.
Gateway IP Address:	Specify the IP address that identifies the ISP server through which your Internet connection will be routed.
PPP *Username:* *Password:*	If you select PPP as the Encapsulation type, enter the Username and Password provided by your ISP.
Use DNS:	Select **Enable** to turn on the DNS forwarding service, which forwards to your LAN PCs the DNS server addresses that your PPP connection learns from your ISP. This option can only be used when the HM210dp/di acts as a DHCP server for your LAN.

Field	Description
DNS *Primary/Secondary DNS Server:*	You may just keep the default 0.0.0.0. If you enter the Primary/Secondary DNS addresses given by your ISP, these DNS servers will be used in addition to any DNS servers discovered automatically.

After completing the required settings, click the **Submit** button.

Then, go to **Admin > Commit & Reboot** and click the **Commit** button to store your changes to permanent memory.

5 Basic Configuration

This chapter provides basic configuration instructions to get your HM210dp/di run and have your network connected to the Internet.

The instructions assume that the HM210dp/di is not predefined with any ATM VC, PPP or IpoA settings. For each connection method, example parameters are given for your better understanding. You should consult with your ISP to determine your connection mode and enter the actual values provided by your ISP.

NOTE! Your HM210dp/di may already be pre-configured with the necessary settings to get your network connected to the Internet. Contact your ISP to determine whether you should change any existing values.

5.1 Configuring the ATM Virtual Circuit

As your LAN computers access the Internet via the HM210dp/di, data is exchanged with your ISP through a complex network of telephone switches, Internet routers, servers, and other specialized hardware. These various devices communicate using a common language, or protocol, called *Asynchronous Transfer Mode (ATM).* On the Wide Area Network (WAN) that connects you to your IPS, the ATM protocol performs functions like those that the Ethernet protocol performs on your LAN.

This section describes how to configure the ATM *Virtual Circuit (VC).* The VC properties define the path the HM210dp/di uses to communicate with your ISP over the ATM network.

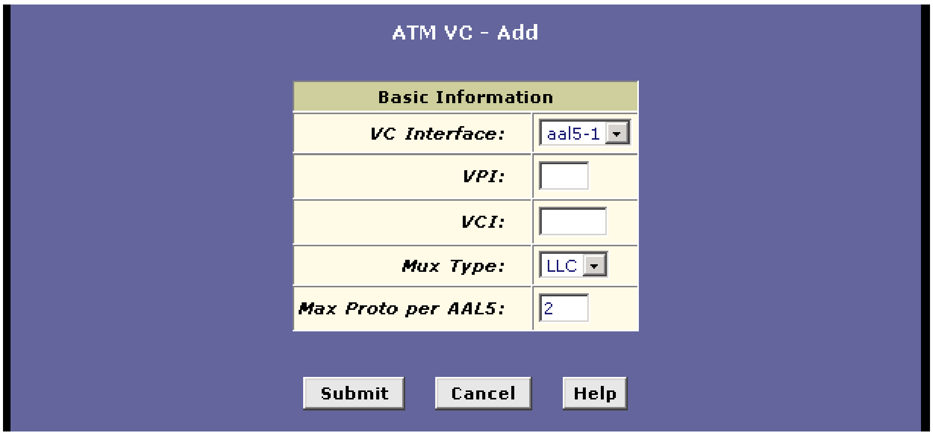
5.1.1 Adding ATM VCs

You may need to create a VC if none has been predefined on your system or if you use multiple services with your ISP. Each service may require its own VC.

Follow these instructions to add an ATM VC Interface:

1. Select **ATM > ATM VC** to display the **ATM VC Configuration** page.

2. Click the **Add** button to display the **ATM VC – Add** page:



ATM VC - Add

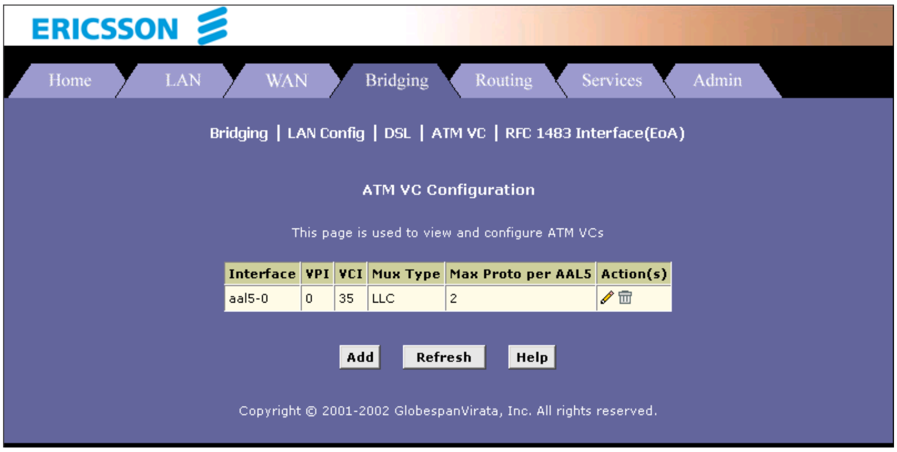
Basic Information	
VC Interface:	aal5-1
VPI:	
VCI:	
Mux Type:	LLC
Max Proto per AAL5:	2

Enter the provided fields as below:

Field	Description
VC Interface:	Select a VC interface from the available interfaces, e.g. **aal5-0**.
VPI and VCI:	Enter the VPI/VCI values given by your ISP, e.g. **0/33**.
Mux Type:	Select **LLC** or **VC** as required by your ISP.
Max Proto per AAL5:	This setting indicates the number of higher-level interfaces that the VC can support (the higher level interfaces can be PPP, EoA, or IpoA interfaces). Contact your ISP to determine wich connection protocol(s) they require.

3. After entering the fields above, click the **Submit** button and when the confirmation page appears, click **Close**.

4. You will return to the **ATM VC Configuration** table and see the newly added ATM VC entry:


ERICSSON
Home
LAN
WAN
Bridging
Routing
Services
Admin
Bridging | LAN Config | DSL | ATM VC | RFC 1483 Interface(EoA)
Add
Refresh
Help

ATM VC Configuration

This page is used to view and configure ATM VCs

Interface	VPI	VCI	Mux Type	Max Proto per AAL5	Action(s)
aal5-0	0	35	LLC	2	✎ 🗑

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

5. Select **Admin > Commit & Reboot** and click the **Commit** button to store your changes to permanent memory.

6. You may need to create a new WAN interface, or modify an existing interface, so that it uses the new VC. See the instructions in the following sections for configuring a PPP (section 5.2), EoA (section 5.3) or IpoA (section 5.4) interfaces, depending on the type you use to communicate with your ISP.

5.1.2 Modifying ATM VCs

Your device may already be preconfigured with the necessary ATM VC properties, or the table may contain placeholder values that you must change before using the device. Contact your ISP to determine your ATM VC values. Follow these instructions to modify a preconfigured VC:

1. From the **ATM VC Configuration** page, click ✎ in the “Actions” column for the interface you want to modify. The **ATM VC Interface – Modify** page displays.

2. Enter the new VPI and VCI values, select the Mux Type, or change the maximum number of protocols that the VC can carry, as directed by your ISP.
   You cannot modify the interface type over which an existing VC operates (aal5-0, for example). If you want to change the interface type, you must delete the existing interface, create a new one, and select the desired interface type.

3. After entering the fields above, click the **Submit** button and when the confirmation page appears, click **Close**.

4. Select **Admin > Commit & Reboot** and click the **Commit** button to store your changes to permanent memory.

5.2 Configuring PPP Interfaces

When powered on, the HM210dp/di initiates a connection through your DSL line to your ISP.

The Point-to-Point (PPP) protocol is commonly used between ISPs and their customers to identify and control various communication properties, including:

- Identifying the type of service the ISP provides to a given customer.
- Identifying the customer to the ISP through a username and password login.
- Enabling the ISP to assign Internet information to the customer's computers.

Your ISP may or may not use the PPP protocol. Contact your ISP to determine if you will need to change the default settings in order to connect to their server.

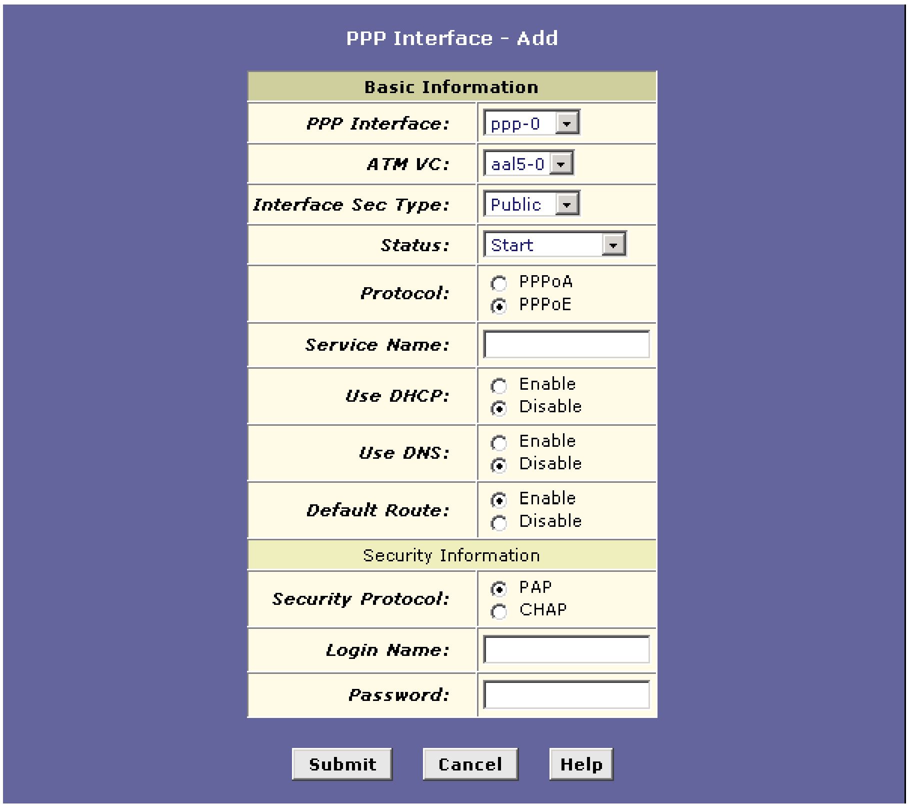
5.2.1 Adding PPP Interfaces

If you intend to use more than one type of service from your ISP, the device can be configured with multiple PPP interfaces, each with unique logon and other properties.

Follow this procedure to define properties for a PPP interface:

1. Select **WAN > PPP** to display the **Point to Point Protocol (PPP) Configuration** page.

2. Click the **Add** button to display the **PPP Interface – Add** page:



PPP Interface - Add

Basic Information	
PPP Interface:	ppp-0
ATM VC:	aal5-0
Interface Sec Type:	Public
Status:	Start
Protocol:	○ PPPoA ● PPPoE
Service Name:	
Use DHCP:	○ Enable ● Disable
Use DNS:	○ Enable ● Disable
Default Route:	● Enable ○ Disable
Security Information	
Security Protocol:	● PAP ○ CHAP
Login Name:	
Password:	

3. Enter the provided fields as below:

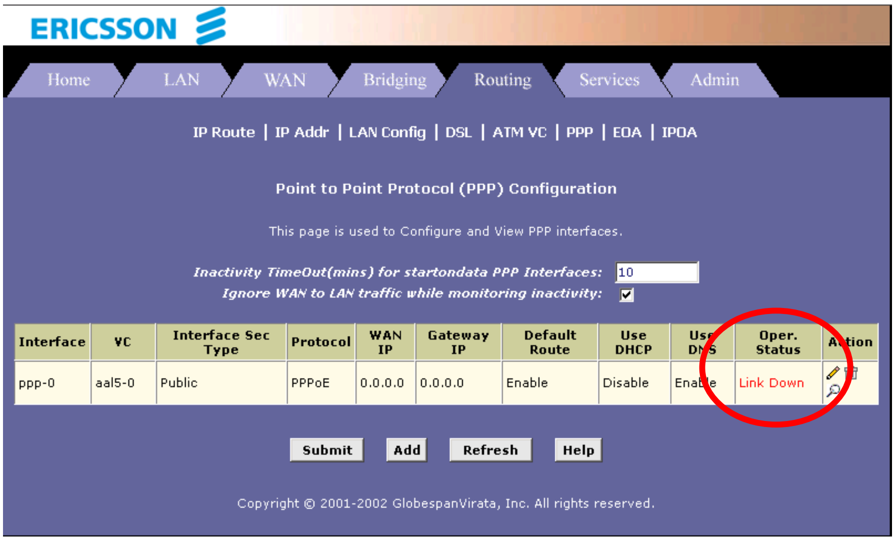
Field	**Description**
PPP Interface:	Select a PPP interface from the available interfaces, e.g. **ppp-0**.
ATM VC:	Select the ATM VC you wish to use for this connection, e.g. **aal5-0**.
Interface Sec Type:	**Public / Private / DMZ**. This setting defines the type of firewall protections that are in effect on the interface as described below: A **public** interface connects to the Internet (PPP interfaces are typically public). Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software.

	A **private** interface connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network. The term **DMZ** (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public Web server). Packets incoming on a DMZ interface – whether from a LAN or external source – are subject to a set of protections that is in between public and private interfaces in terms of restrictiveness.
Status:	**Start** – To establish a connection whenever you turn on the HM210dp/di. **StartOnData** – To establish a connection whenever the device gets a request to connect to the Internet, such as when you open a browser requesting for web pages.
Protocol:	**PPPoA** or **PPPoE** as required by your ISP.
Service Name:	ISPs may offer different types of services (for example, for online gaming or business communications), each requiring a different login and other connection properties. For **PPPoA** no need to set up. For **PPPoE** enter the Service Name if this is required by your ISP. Otherwise leave it blank.
Use DHCP:	When set to **Enable**, the device will acquire additional IP information from the ISP's DHCP server. The PPP connection itself acquires the device's IP address, mask, DNS address, and default gateway address. When enabled, the device will acquire IP addresses for various other server types (WINS, SMTP, POP3, etc).
Use DNS:	When set to **Enable**, the DNS address learned through the PPP connection will be distributed to clients of the device's DHCP server. This option is useful only when the HM210dp/di is configured to act as a DHCP server for your LAN.
Default Route:	Indicates whether the HM210dp/di should use the IP address assigned to this connection as its default route.

Security Information *Security Protocol:*	Select **PAP** or **CHAP** as required by your ISP.
Login Name: *Password:*	The login name and password given by your ISP. **NOTE** that characters of colon (:), semicolon (;) and questions mark (?) are not allowed when entering login name and password.

5. After entering the fields above, click the **Submit** button and when the confirmation page appears, click **Close**.

6. You will return to the **PPP Configuration** page and see the newly added PPP interface. The “Oper. Status” column indicates if the link is currently up or down:



Point to Point Protocol (PPP) Configuration

This page is used to Configure and View PPP interfaces.

Inactivity TimeOut(mins) for startondata PPP Interfaces: 10
Ignore WAN to LAN traffic while monitoring inactivity: ☑

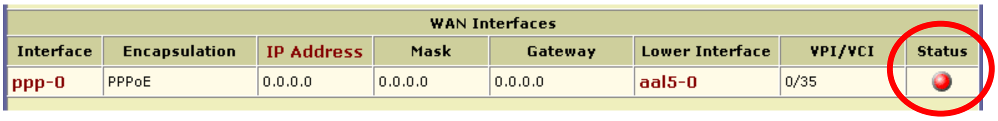
Interface	VC	Interface Sec Type	Protocol	WAN IP	Gateway IP	Default Route	Use DHCP	Use DNS	Oper. Status	Action
ppp-0	aal5-0	Public	PPPoE	0.0.0.0	0.0.0.0	Enable	Disable	Enable	Link Down	

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

7. Select **Admin > Commit & Reboot** and click the **Commit** button to store your changes to permanent memory.

5.2.2 Checking Your Connection Status

Select **Home > System Mode**. The “WAN Interface” item should display the interface you created to communicate with your ISP. A green ball in the “Status” field indicates a successful connection:



WAN Interfaces

Interface	Encapsulation	IP Address	Mask	Gateway	Lower Interface	VPI/VCI	Status
ppp-0	PPPoE	0.0.0.0	0.0.0.0	0.0.0.0	aal5-0	0/35	●

5.2.3 Modifying and Deleteing PPP Interfaces

To modify a PPP interface, display the **PPP Configuration** page and click ✏ in the “Action(s)” column for the interface you want to modify. The **PPP Interface – Modify** page displays.

You can change only the status of the PPP connection, the security protocol, your login name and your password. To modify the other settings, you must delete the interface and create a new one.

To delete a PPP interface, display the **PPP Configuration** page and click 🗑 in the “Action(s)” column for the interface you want to delete. You should not delete a PPP interface unless you have received instructions to do so from your ISP. Without an appropriately defined PPP interface, you may not be able to connect to your ISP. You can recreate the PPP interface with the same name at a later time.

After modifying or deleting a PPP interface, click the **Submit** button. Then select **Admin > Commit & Reboot** and click the **Commit** button to save your changes to permanent memory.

5.3 Configuring EoA Interfaces

This section describes how to configure an Ethernet-over-ATM interface on the HM210dp/di, if one is needed to communicate with your ISP.

The Ethernet-over-ATM (EoA) protocol is often referred to as *RFC1483,* which is the Internet specification that defines it. It is commonly used to carry data between local area networks that use the Ethernet protocol and wide-area networks that use the ATM protocol. Many telecommunications industry networks use the ATM protocol. ISPs who provide DSL services often use the EoA protocol for data transfer with their customers' DSL modems.

EoA can be implemented to provide a bridged connection between a DSL modem and the ISP. In a bridged connection, data is shared between the ISP's network and their customer's as if the networks were on the same physical LAN. Bridged connections do not use the IP protocol. EoA can also be configured to provide a routed connection with the ISP, which uses the IP protocol to exchange data.

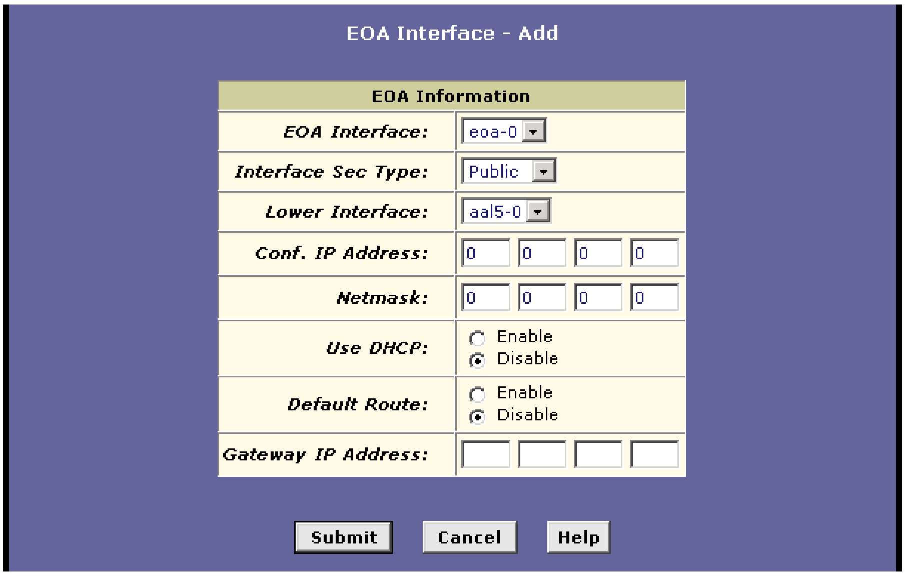
Before creating an EoA interface or modifying the default settings, contact your ISP to determine which type of protocol they use.

5.3.1 Adding EoA Interfaces

Follow these instructions to add an EoA interface:

1. Select **WAN > EoA** to display the **RFC1483/Ethernet over ATM(EoA) Configuration** page.

2. Click the **Add** button to display the **EOA Interface – Add** page:



EOA Interface - Add

EOA Information	
EOA Interface:	eoa-0
Interface Sec Type:	Public
Lower Interface:	aal5-0
Conf. IP Address:	0 . 0 . 0 . 0
Netmask:	0 . 0 . 0 . 0
Use DHCP:	○ Enable ● Disable
Default Route:	○ Enable ● Disable
Gateway IP Address:	

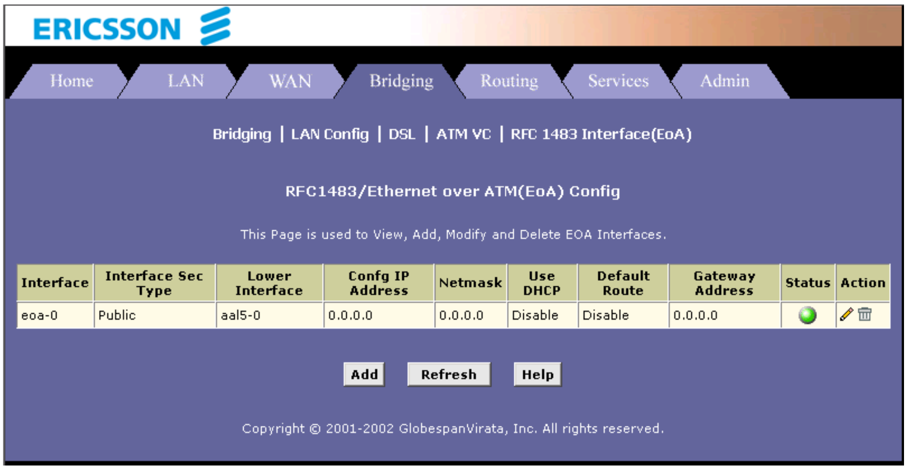
3. Enter the provided fields as below:

Field	Description
EOA Interface:	Select an EoA interface from the available interfaces, e.g. **eoa-0**.
Interface Sec Type:	**Public / Private / DMZ**. This setting defines the type of firewall protections that are in effect on the interface as described below: A **public** interface connects to the Internet (PPP interfaces are typically public). Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software. A **private** interface connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network. The term **DMZ** (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses

	(such as a company's public Web server). Packets incoming on a DMZ interface – whether from a LAN or external source – are subject to a set of protections that is in between public and private interfaces in terms of restrictiveness.
Lower Interface:	Select an ATM VC interface previously created, e.g. **aal5-0**. EoA interfaces are defined in software, and then associated with lower-level software and hardware structures (at the lowest level, they are associated with a physical port – the WAN port). This field should reflect an interface name defined in the next lower level of software over which the EoA interface will operate.
Conf. IP Address: *Netmask:*	**0.0.0.0 / 0.0.0.0** To use the HM210dp/di as a bridge, you don't need to set the IP address and subnet mask. Just keep the default.
Use DHCP:	**Enable / Disable** When **Enabled**, this setting instructs the device to accept IP information assigned dynamically by your ISP's DHCP server. If the interface will be used for bridging with your ISP and you will not be routing data through it, leave this checkbox unselected.
Default Route:	**Enable / Disable** Indicates whether the HM210dp/di uses the IP address assigned to this interface, if any, as its default route for your LAN. Your system can have only one default route.
Gateway IP Address:	The external IP address that the HM210dp/di communicates with via the EoA interface to gain access to the Internet. This is typically an ISP server.

4. After entering the fields above, click the **Submit** button and when the confirmation page appears, click **Close**.

5. You will return to the **EoA Configuration** page and see the newly added EoA interface:


ERICSSON
Home
LAN
WAN
Bridging
Routing
Services
Admin
Bridging | LAN Config | DSL | ATM VC | RFC 1483 Interface(EoA)

RFC1483/Ethernet over ATM(EoA) Config

This Page is used to View, Add, Modify and Delete EOA Interfaces.

Interface	Interface Sec Type	Lower Interface	Confg IP Address	Netmask	Use DHCP	Default Route	Gateway Address	Status	Action
eoa-0	Public	aal5-0	0.0.0.0	0.0.0.0	Disable	Disable	0.0.0.0	●	✎ 🗑

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

6. Select **Admin > Commit & Reboot** and click the **Commit** button to store your changes to permanent memory.

5.4 Configuring IPoA Interfaces

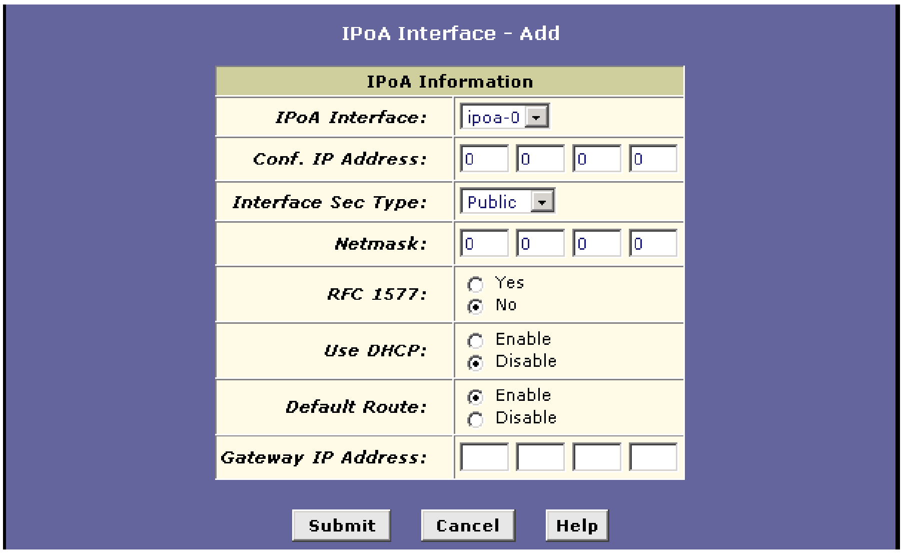
This section describes how to configure an IPoA (Internet Protocol-over-ATM) interface on the HM210dp/di.

An IPoA interface can be used to exchange IP packets over the ATM network, without using an underlying Ethernet over ATM (EoA) connection. Typically, this type of interface is used only in product development and test environments, to eliminate unneeded variables when evaluating IP layer processing.

5.4.1 Adding IPoA Interfaces

Follow these instructions to add an IPoA interface:

1. Select **WAN > IPoA** to display the **IPoA Configuration** page.
2. Click the **Add** button to display the **IPoA Interface – Add** page:



IPoA Interface - Add

IPoA Information	
IPoA Interface:	ipoa-0
Conf. IP Address:	0 . 0 . 0 . 0
Interface Sec Type:	Public
Netmask:	0 . 0 . 0 . 0
RFC 1577:	○ Yes ● No
Use DHCP:	○ Enable ● Disable
Default Route:	● Enable ○ Disable
Gateway IP Address:	

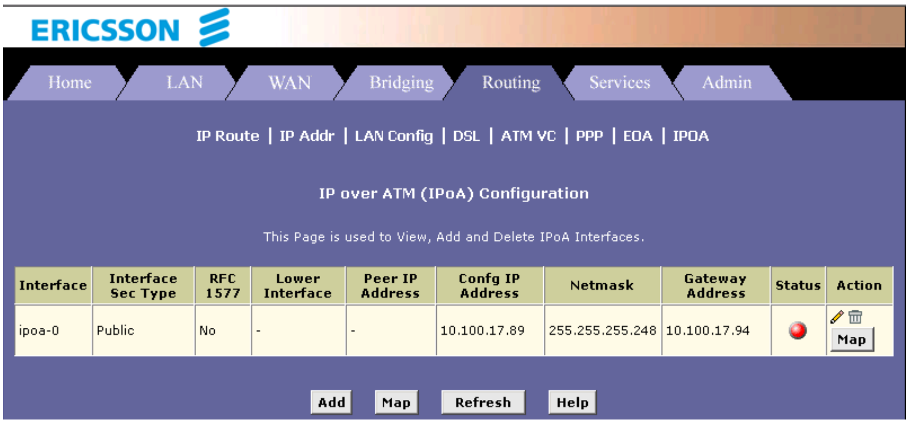
3. Enter the provided fields as below:

Field	Description
IPoA Interface:	Select an IPoA interface from the available interfaces, e.g. **ipoa-0**.
Conf. IP Address:	Enter the IP address given by your ISP.

Interface Sec Type:	**Public / Private / DMZ**. This setting defines the type of firewall protections that are in effect on the interface as described below: A **public** interface connects to the Internet (PPP interfaces are typically public). Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software. A **private** interface connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network. The term **DMZ** (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public Web server). Packets incoming on a DMZ interface – whether from a LAN or external source – are subject to a set of protections that is in between public and private interfaces in terms of restrictiveness.
Netmask:	Enter the IP address given by your ISP.
RFC 1577:	Specifies whether the IPoA protocol to be used complies with the IEFT specification named "RFC 1577 – Classical IP and ARP over ATM". Select **Yes** for RFC 1577-Classical IP and ARP over ATM. Select **No** for RFC 1483 Router.
Use DHCP:	**Enable / Disable** When **Enabled**, this setting instructs the device to accept IP information assigned dynamically by your ISP's DHCP server. If the interface will be used for bridging with your ISP and you will not be routing data through it, leave this checkbox unselected.
Default Route:	**Enable / Disable** Indicates whether the HM210dp/di uses the IP address assigned to this interface, if any, as its default route for your LAN. Your system can have only one default route.
Gateway IP Address:	Enter the gateway IP address given by your ISP.

4. After entering the fields above, click the **Submit** button and when the confirmation page appears, click **Close**.

5. You will return to the **IpoA Configuration** table and see the newly added IPoA entry:

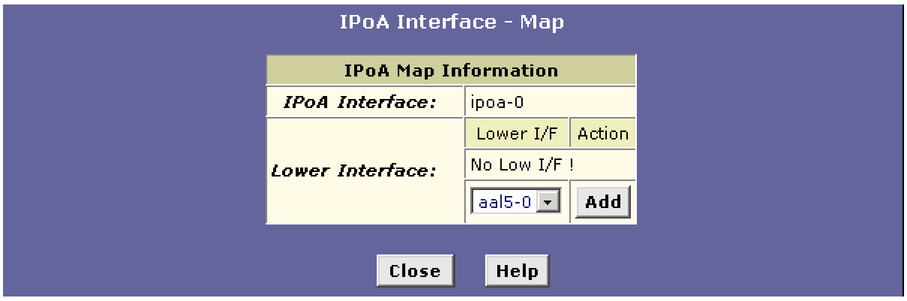

ERICSSON
Home
LAN
WAN
Bridging
Routing
Services
Admin
IP Route | IP Addr | LAN Config | DSL | ATM VC | PPP | EOA | IPOA

IP over ATM (IPoA) Configuration

This Page is used to View, Add and Delete IPoA Interfaces.

Interface	Interface Sec Type	RFC 1577	Lower Interface	Peer IP Address	Config IP Address	Netmask	Gateway Address	Status	Action
ipoa-0	Public	No	-	-	10.100.17.89	255.255.255.248	10.100.17.94	●	Map

6. Click **Map** in the "Action" column. The **IPoA Interface – Map** page appears:


IPoA Interface - Map

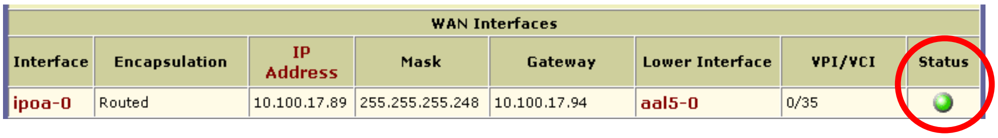
IPoA Map Information		
IPoA Interface:	ipoa-0	
Lower Interface:	Lower I/F	Action
	No Low I/F !	
	aal5-0	Add

7. Select an ATM VC you have created earlier from the "*Lower Interface:"* dropdown list and then click **Add**. Click **Close** to exit the confirmation page.

8. Select **Admin > Commit & Reboot** and click the **Commit** button to store your changes to permanent memory.

5.4.2 Checking Your Connection Status

Select **Home > System Mode**. The WAN Interface item should display the interface you created to communicate with your ISP. A green ball in the Status field indicates a successful connection:


WAN Interfaces

Interface	Encapsulation	IP Address	Mask	Gateway	Lower Interface	VPI/VCI	Status
ipoa-0	Routed	10.100.17.89	255.255.255.248	10.100.17.94	aal5-0	0/35	●

5.5 Bridging Connection Mode

The HM210dp/di can be configured to act as a bridging device between your LAN and your ISP. Bridges are devices that enable two or more networks to communicate as if they are two segments of the same physical LAN.

Although the HM210dp/di is preconfigured to serve as router for providing Internet connectivity to your LAN, there are several instances in which you may also want to configure bridging:

- ❑ Your ISP may use protocols that require bridging with your LAN. The device can be configured to appear as a bridge when communicating with your ISP, while continuing to provide router functionality for your LAN.
- ❑ Your LAN may include computers that communicate using “layer-3” protocols other than the Internet Protocol. These include IPX® and AppleTalk®. In this case, the device can be configured to act as a bridge for packets that use these protocols while continuing to serve as a router for IP data.

5.5.1 Defining Bridge Interfaces

To enable bridging, you simply specify the device interfaces on which you want to bridge data, and then enable bridging mode.

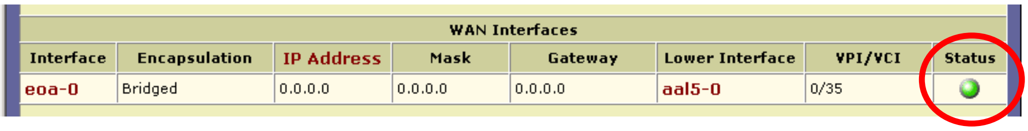
Follow the steps below to enable bridging mode:

1. Select **Bridging > Bridging** page to display the **Bridge Configuration** page.
2. Select the interface names on which you ant to perform bridging and click the **Add** button.

   If you do not have an eoa-0 interface, but instead have an interface named ppp-0 or ipoa-0, your device is not currently configured with a WAN interface that allows bridging with your ISP. Check with your ISP to determine whether they use the eoa protocol before changing this setting.
3. Click the Bridging: Enable radio button to turn on bridging and click the **Submit** button. A page will briefly display to confirm your changes, and will return you to the **Bridge Configuration** page.
4. Select **Admin > Commit & Reboot** and click the **Commit** button to store your changes to permanent memory.

5.5.2 Check Your Connection Status

Select **Home > System Mode**. The WAN Interface item should display the interface you created to communicate with your ISP. A green ball in the Status field indicates a successful connection:



WAN Interfaces

Interface	Encapsulation	IP Address	Mask	Gateway	Lower Interface	VPI/VCI	Status
eoa-0	Bridged	0.0.0.0	0.0.0.0	0.0.0.0	aal5-0	0/35	●

5.5.3 Deleting a Bridge Interface

To make an interface non-bridgeable, display the **Bridge Configuration** page and click 🗑 next to the interface you want to delete.

Click **OK** to confirm the deletion.

The interface remains defined in the system, but is no longer capable of performing bridging.

6 Configuring IP Routes

You can use the Configuration Manager to define specific routes for your Internet and network data. This chapter provides instructions for creating routes.

Most users do not need to define IP routes. On a typical small home or office LAN, the existing routes that set up the default gateways for your LAN computers and for the HM210dp/di provide the most appropriate path for all your Internet traffic. You may need to define routes if:

- Your network setup includes two or more networks or subnets.
- You connect to two or more ISP services.
- You connect to a remote corporate LAN.

6.1 Overview of IP Routes

The essential challenge of a router is: when it receives data intended for a particular destination, which next device should it send that data to? When you define IP routes, you provide the rules that a computer uses to make these decisions.

Each time Internet data is passed from one Internet address to another, it is said to take a *hop*. A hop can be a handoff to a different port on the same device, to a different device on the same network, or to a device on an entirely different network.

When a hop passes data from one type of network to another, it uses a *gateway*. A gateway is an IP address that provides initial access to a network, just as a switchboard serves as a gateway to a specific set of phone numbers. For example, when a computer on your LAN requests access to a company’s web site, your ISP serves as a gateway to the Internet. As your request reaches its destination, another gateway provides access to the company’s web servers.

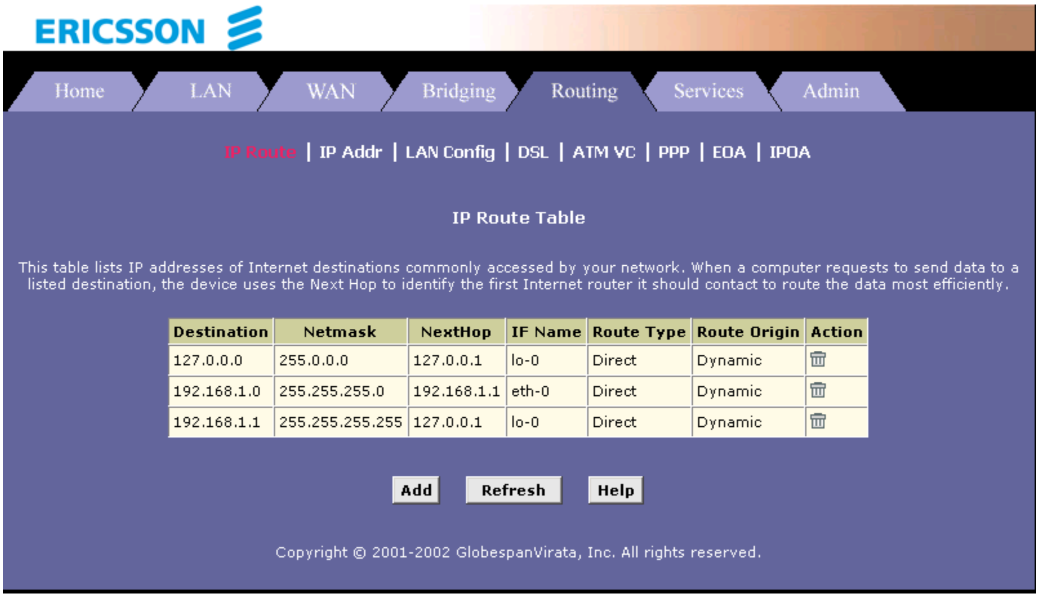
IP routes are defined on computers, routers, and other IP-enabled devices to instruct them which hop to take, or which gateway to use, to help forward data along to its specified destination.

If no IP route is defined for a destination, then IP data is passed to a predetermined *default gateway*. The default gateway serves like a higher-level telephone switchboard; it may not be able to connect directly to the destination, but it will know a set of other devices that can help pass the data intelligently. If it cannot determine which of these devices provides a good next hop (because no such route has been defined), then that device will forward the data to *its* default gateway. Eventually, a high level device, using a predefined IP route, will be able to forward the data along a path to its destination.

6.2 Viewing the IP Routing Table

All IP-enabled computers and routers maintain a table of IP addresses that are commonly accessed by their users. For each of these *destination IP addresses*, the table lists the IP address of the first hop the data should take. This table is known as the device's *routing table*.

To view the HM210dp/di routing table, select **Routing > IP Route**. The following page appears:


ERICSSON
Home
LAN
WAN
Bridging
Routing
Services
Admin
IP Route | IP Addr | LAN Config | DSL | ATM VC | PPP | EOA | IPOA
Add
Refresh
Help

IP Route Table

This table lists IP addresses of Internet destinations commonly accessed by your network. When a computer requests to send data to a listed destination, the device uses the Next Hop to identify the first Internet router it should contact to route the data most efficiently.

Destination	Netmask	NextHop	IF Name	Route Type	Route Origin	Action
127.0.0.0	255.0.0.0	127.0.0.1	lo-0	Direct	Dynamic	🗑
192.168.1.0	255.255.255.0	192.168.1.1	eth-0	Direct	Dynamic	🗑
192.168.1.1	255.255.255.255	127.0.0.1	lo-0	Direct	Dynamic	🗑

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

The **IP Route Table** displays a row for each existing route. These include routes that were predefined on the device, routes you may have added, and routes that the device has identified automatically through communication with other devices.

The routing table should reflect a default gateway, which directs outbound Internet traffic to your ISP. This default gateway is shown in the row containing destination address 0.0.0.0.

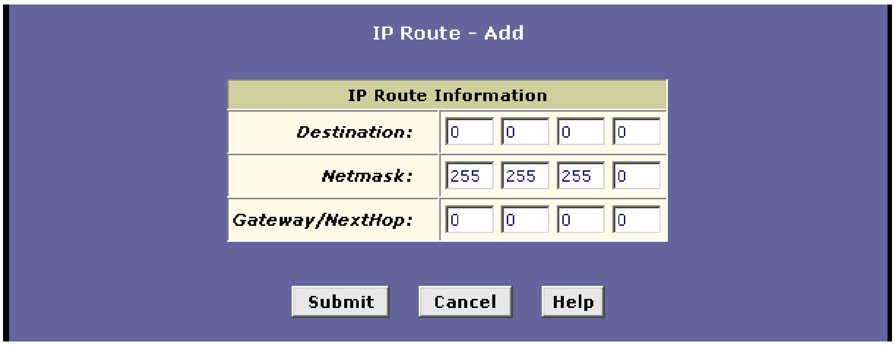
The following table defines the fields in the IP Routing table:

Field	Description
Destination:	Specifies the IP address of the destination computer. The destination can be specified as the IP address of a specific computer or an entire network. It can also be specified as all zeros to indicate that this route should be used for all destinations for which no other route is defined (this is the route that creates the default gateway).
Netmask:	Indicates which parts of the destination address refer to the network and which parts refer to a computer on the network. The default gateway uses a netmask of 0.0.0.0.
NextHop	Specifies the *next* IP address to send data to when its final destination is that shown in the destination column.
IFName:	Displays the name of the interface on the device through which data is forwarded to the specified next hop.
Route Type:	Displays whether the route is direct or indirect. In a *direct* route, the source and destination computers are on the same network, and the router attempts to directly deliver the data to the computer. In an *indirect* route, the source and destination computers are on different networks, and the router forwards data to a device on another network for further handling.
Route Origin:	Displays how the route was defined. *Dynamic* indicates that the route was created automatically or predefined by your ISP or the manufacturer. Routes you create are labeled *Local*. Other routes can be created automatically (using RIP), or defined remotely through various network management protocols (LCL or ICMP).
Action:	Displays and icon (🗑) you can click to delete a route.

6.3 Adding IP Routes

To add an IP route to the routing table, follow the steps below:

1. Select **Routing > IP Route > Add**. The **IP Route – Add** page appears:



IP Route - Add

IP Route Information				
Destination:	0	0	0	0
Netmask:	255	255	255	0
Gateway/NextHop:	0	0	0	0

2. Specify the destination, netmask, and gateway or next hop for this route. For a description of these fields, refer to the table on the previous page.

   To create a route that defines the default gateway for your LAN, enter **0.0.0.0** in both the **Destination** and **Netmask** fields. Enter your ISP's IP address in the **Gateway/NextHop** field.

   NOTE! You cannot specify the interface name, route type or route origin. These parameters are used only for routes that are identified automatically as the device communicates with other routing devices. For routes you create, the routing table displays system default values in these fields.

3. Click the **Submit** button. The IP routing Table will now display the new route.

4. Select **Admin > Commit & Reboot** and click the **Commit** button to save your changes to permanent storage.

7 Configuring DHCP

You can configure your network and HM210dp/di to use the Dynamic Host Configuration Protocol (DHCP). This chapter provides instructions for implementing DHCP on your network.

7.1 Overview of DHCP

DHCP is a protocol that enables network administrators to centrally manage the assignment and distribution of IP information to computers on a network.

When you enable DHCP on a network, you allow a device – such as the HM210dp/di or a router located with your ISP – to assign temporary IP addresses to your computers whenever they connect to your network. The assigning device is called a *DHCP Server* and the receiving device is a *DHCP Client*.

The DHCP server draws from a defined pool of IP addresses and “leases” them for a specified amount of time to your computers when they request an Internet session. It monitors, collects, and redistributes the addresses as needed.

On a DHCP-enabled network, the IP information is assigned *dynamically* rather than *statically*. A DHCP client can be assigned a different address from the pool each time it reconnects to the network.

DHCP allows you to manage and distribute IP addresses throughout your network from a central computer. Without DHCP, you would have to configure each computer separately with IP addresses and related information. DHCP is commonly used with large networks and those that are frequently expanded or otherwise updated

7.2 DHCP Modes

The HM210dp/di can be configured as a DHCP server, DHCP relay agent, or in some cases, a DHCP client.

- ❑ **DHCP Server**
  The HM210dp/di will maintain the pool of addresses and distribute them to your LAN computers. If the pool of addresses includes private IP addresses, you must also configure the Network Address Translation (NAT) service, so that the private addresses can be

translated to your public IP address on the Internet. Both DHCP server and NAT are enabled in the default configuration.

- **DHCP Relay Agent**
  If your ISP performs the DHCP server function for your network, then you can configure the HM210dp/di as a DHCP relay agent. When the HM210dp/di receives a request for Internet access from a computer on your network, it contacts your ISP for the necessary IP information, and then relays the assigned information back to the computer.

- **DHCP Client**
  If you have another PC or device on your network that is already performing the DHCP server function, you can configure the LAN port on the HM210dp/di to be a DHCP client of that server.

NOTE! Your can input settings for both DHCP server and DHCP relay mode, and then activate either mode at any time. Deactivated settings are retained for your future use.

7.3 Configuring DHCP Server

To set up DHCP server, you first define the ranges of IP addresses that you want to be distributed to your PCs, called DHCP server address pools.

IP address pools can contain multiple public addresses that you have purchased from your ISP, but are typically private addresses that you create. LAN administrators often create private IP addresses for use only on their networks. See “Overview of NAT” for an explanation of private IP addresses.

You can create up to two pools and the pools can maintain a combined total of 254 IP addresses. For example, you could configure only one pool with addresses in the range 192.168.1.2 through 192.168.1.255, or two pools with the following address range:
Pool 0: 192.168.1.2 through 192.168.1.128
Pool 1: 192.168.1.129 through 192.168.1.255

You may want to create a second pool if any of these circumstances apply:

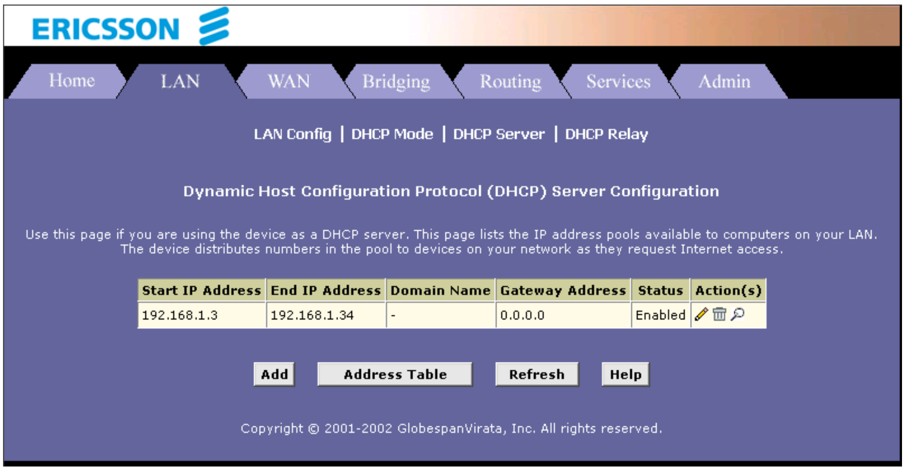
- Your LAN configuration includes two subnets.

- You have only one subnet, but the addresses you want to distribute are not in a continuous range.

7.3.1 Creating DHCP Server Address Pools

To create a pool of IP addresses follow the steps below:

1. Select **LAN > DHCP Server**. The **DHCP Server Configuration** page appears:



Dynamic Host Configuration Protocol (DHCP) Server Configuration

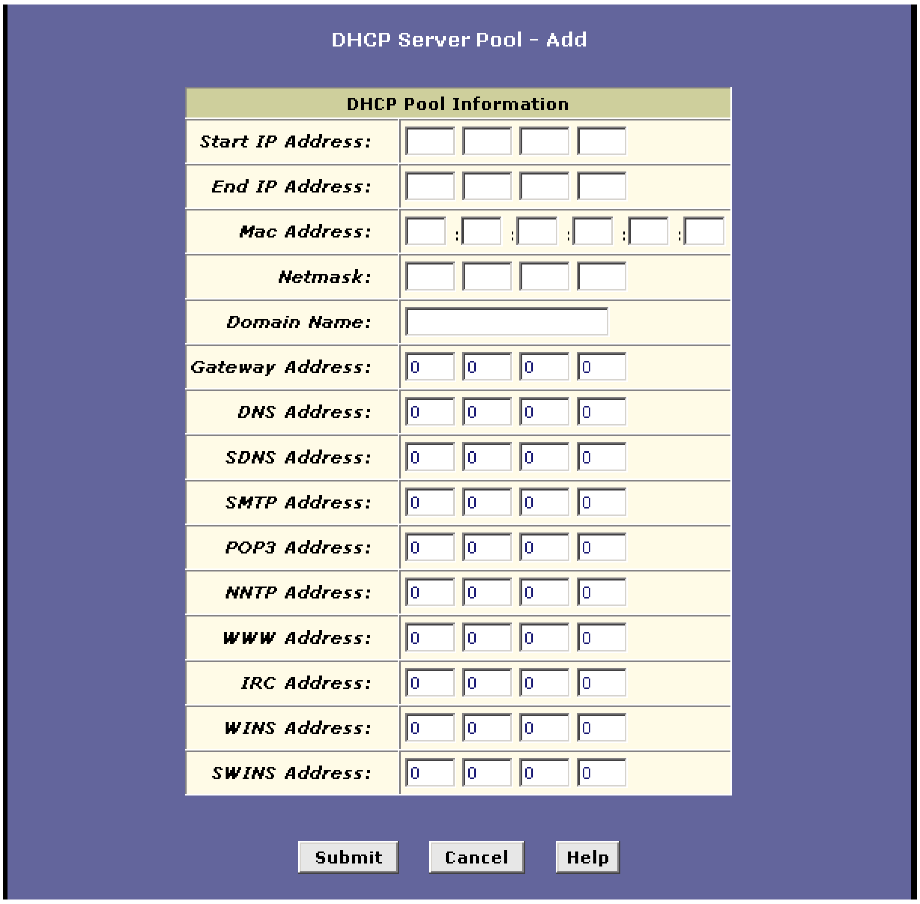
Use this page if you are using the device as a DHCP server. This page lists the IP address pools available to computers on your LAN. The device distributes numbers in the pool to devices on your network as they request Internet access.

Start IP Address	End IP Address	Domain Name	Gateway Address	Status	Action(s)
192.168.1.3	192.168.1.34	-	0.0.0.0	Enabled	

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Depending on your preconfigured settings, the table may display one or more address pools, each in a row, or may be empty.

2. To add an IP address pool, click **Add**. The **DHCP Server Pool – Add** page appears:



DHCP Server Pool - Add

DHCP Pool Information	
Start IP Address:	
End IP Address:	
Mac Address:	: : : : :
Netmask:	
Domain Name:	
Gateway Address:	0 0 0 0
DNS Address:	0 0 0 0
SDNS Address:	0 0 0 0
SMTP Address:	0 0 0 0
POP3 Address:	0 0 0 0
NNTP Address:	0 0 0 0
WWW Address:	0 0 0 0
IRC Address:	0 0 0 0
WINS Address:	0 0 0 0
SWINS Address:	0 0 0 0

Enter the provided fields as below:
The **Start IP Address**, **End IP Address**, **Net Mask** and **Gateway Address** fields are required, the others are optional.

Field	**Description**
Start IP Address: *End IP Address:*	Specify the lowest and highest IP addresses in the pool, up to a maximum range of 254 addresses. For example, if the LAN port is assigned IP address 192.168.1.1, then you could create a pool with address range 192.168.1.2 – 192.168.1.254 for distribution to your LAN computers.
Mac Address:	A MAC address is a manufacturer-assigned hardware ID that is unique for each device on a network. Use this field only if you want to assign a specific IP address to the computer that uses this MAC address. If you type a MAC address here, you must have specified the same IP

	address in both the Start/End IP Address fields.
Netmask:	Specifies which portion of each IP address in this range refers to the network and which portion refers to the host (computer). You can use the network mask to distinguish which pool of addresses should be distributed to a particular subnet.
Domain Name:	A user-friendly name that refers to the subnet that includes the addresses in this pool. This is used for reference only.
Gateway Address:	The address of the default gateway for computers that receive IP addresses from this pool. If no value is specified, then the appropriate LAN (eth-0) port address on the device will be distributed to each PC as its gateway address.
DNS/SDNS Address:	The IP address of the *Domain Name System* server and *Secondary Domain Name System* server to be used by computers that receive IP addresses from this pool. These DNS servers translate common Internet names that you type into your web browser into their equivalent numeric IP addresses. Typically, these servers are located with your ISP.
SMTP … SWINS Address: (optional)	The IP addresses of devices that perform various services for computers that receive IP addresses from this pool (such as the SMTP, or *Simple Mail Transfer Protocol,* server which handles e-mail traffic). Contact your ISP for these addresses.

3. Click the **Submit** button. A confirmation page appears briefly to indicate that the pool has been added successfully. After a few seconds, the **DHCP Server Pool – Add** page displays with the newly added pool.

4. Follow the instructions in the next section to enable the DHCP Server mode.

7.3.2 Enabling DHCP Server Mode

To enable the DHCP server mode follow the steps below:

1. Select **LAN > DHCP Mode** and from the “DHCP Mode” dropdown list select **DHCP Server**. Click the **Submit** button.

2. A page appears to confirm the change.

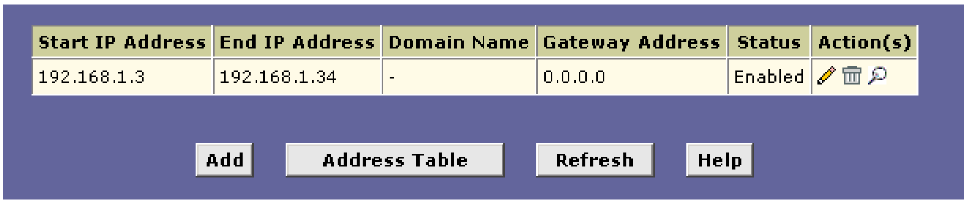
3. Select **Admin > Commit & Reboot** and click the **Commit** button to save your changes to permanent storage.

7.3.3 Configuring Your PCs as DHCP Clients

For each computer that you want to configure to receive IP information automatically, configure the TCP/IP properties to “Obtain an IP address automatically” (the actual text may vary depending on your operating system). Refer to section 3.1 “Configuring your PCs as DHCP Clients” for detailed instructions.

7.3.4 Viewing, Modifying and Deleting Address Pools

To view, modify, or delete an existing address pool, display the DHCP Service Configuration page, and click the icons (in the “Action(s)”) column for the corresponding row in the address pool table.

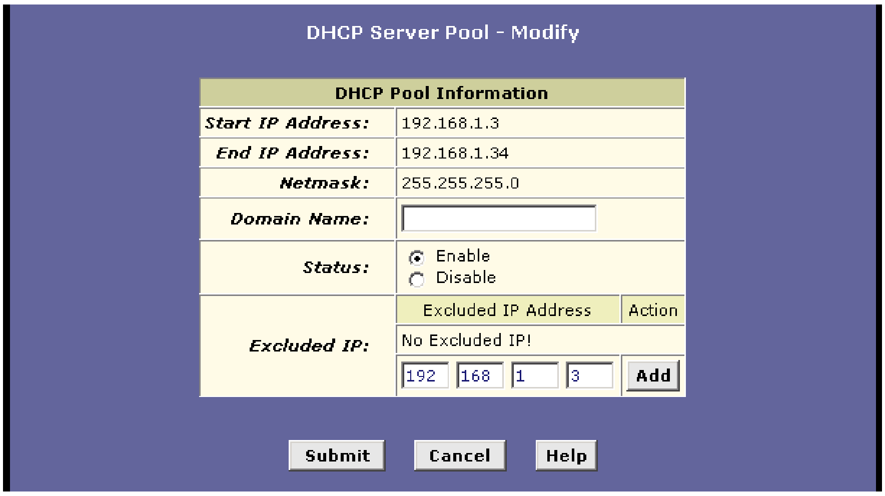


Start IP Address	End IP Address	Domain Name	Gateway Address	Status	Action(s)
192.168.1.3	192.168.1.34	-	0.0.0.0	Enabled	✎ 🗑 🔍

- To delete an IP address pool, click 🗑, then submit and commit your changes.

- To view details on an IP address pool, click 🔍. A page displays with the same information that you entered when you added the pool.

- To modify the pool, click ✎**.** The **DHCP Server Pool – Modify** page displays:



DHCP Server Pool - Modify

DHCP Pool Information	
Start IP Address:	192.168.1.3
End IP Address:	192.168.1.34
Netmask:	255.255.255.0
Domain Name:	
Status:	● Enable ○ Disable
Excluded IP:	Excluded IP Address / Action No Excluded IP! 192 . 168 . 1 . 3 Add

When modifying an IP address pool, you are **only** allowed to:

- Change the domain name associated with the pool and to exclude IP addresses within its range from distribution. To exclude an IP address, enter it in the field provided and click **Add**.

- If you want to change other attributes, you must delete the pool and create a new one.

After entering your changes, click the **Submit** button.

Select **Admin > Commit & Reboot** and click the **Commit** button to save your changes to permanent storage.

7.3.5 Excluding IP Addresses from a Pool

If you have IP addresses that are designated for fixed use with specific devices, or for some other reason you do not want to make them available to your network, you can exclude them from the pool.

Display the **DHCP Server Pool – Modify** page. Type each address to be excluded in the *"Excluded IP:"* field and click **Add**. When you are done specifying excluded addresses, click the **Submit** button.

Select **Admin > Commit & Reboot** and click the **Commit** button to save your changes to permanent storage.

7.3.6 Viewing Current DHCP Address Assignments

When the HM210dp/di functions as a DHCP server for your LAN, it keeps a record of any addresses currently leased to your computers.

To view a table of all current IP address assignments, select **LAN > DHCP Server** and on that page click the **Address Table** button to view the **DHCP Server Address Table** page.

For each leased address, the table lists the following information:

Field	Description
IP Address:	The address that has been leased from the pool.
Netmask:	The network mask associated with the leased address. This identifies the network ID and host ID portions of the address.
Mac Address:	The unique hardware ID of the computer to which the IP address has been assigned.
Pool Start:	The lower boundary of the address pool (shown here to identify the pool from which the leased address was assigned).
Address Type:	Can be *Static* or *Dynamic. Static* indicates that the IP address has been assigned permanently to the specific hardware device. *Dynamic* indicates that the IP address has been leased temporarily for a specified length of time.
Time Remaining:	The amount of time left for the device to use the assigned address. The default lease time is 30 days (31536000 seconds).

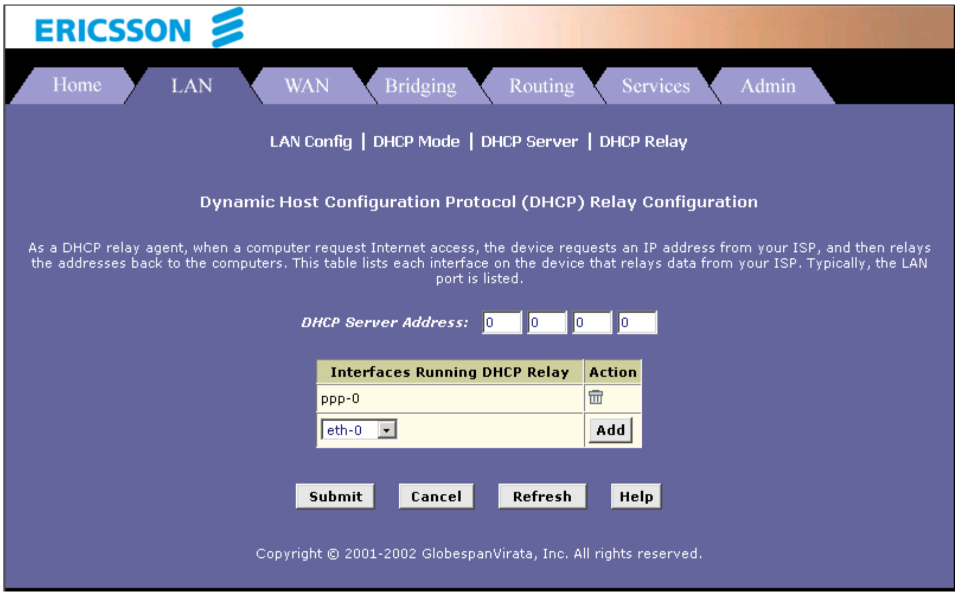
7.4 Configuring DHCP Relay

Some ISPs perform the DHCP server function for their customers' home/small office networks. In this case, you can configure the device as a DHCP relay agent. When a computer on your network requests Internet access, the HM210dp/di contacts your ISP to obtain an IP address (and other information), and then forwards that information to the computer.

7.4.1 Defining the DHCP Relay Interface(s)

To define the DHCP Relay interface(s) follow the steps below:

1. Select **LAN > DHCP Relay**. The **DHCP Relay Configuration** page appears:



Dynamic Host Configuration Protocol (DHCP) Relay Configuration

As a DHCP relay agent, when a computer request Internet access, the device requests an IP address from your ISP, and then relays the addresses back to the computers. This table lists each interface on the device that relays data from your ISP. Typically, the LAN port is listed.

DHCP Server Address: 0 . 0 . 0 . 0

Interfaces Running DHCP Relay	Action
ppp-0	🗑
eth-0 ▾	Add

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

This page provides a text box for entering the IP address of your ISP's DHCP server and a table that lists the interfaces on your HM210dp/di that can relay DHCP information.

2. Type the IP address of your ISP's DHCP server in the fields provided.
   If you do not have this address, it is not essential to enter it. Requests for IP information from your LAN will be passed to the default gateway, which should route the request appropriately.

3. If the interface named **eth-0** is not already displaying, select it from the dropdown list and click **Add** in the "Action" column.

4. Click the **Submit** button. A page appears to confirm your changes and then the program returns to the DHCP Relay Configuration page.

5. Follow the instructions in the next section to enable the DHCP Relay mode.

7.4.2 Enabling DHCP Relay Mode

To enable the DHCP relay mode follow the steps below:

1. Select **LAN > DHCP Mode** and from the "DHCP Mode" dropdown list select **DHCP Relay**. Click the **Submit** button.

2. A page appears to confirm the change.

3. Select **Admin > Commit & Reboot** and click the **Commit** button to save your changes to permanent storage.

7.4.3 Configuring Your PCs as DHCP Clients

For each computer that you want to configure to receive IP information automatically, configure the TCP/IP properties to “Obtain an IP address automatically” (the actual text may vary depending on your operating system). Refer to section 3.1 “Configuring your PCs as DHCP Clients” for detailed instructions.

8 Configuring NAT

This chapter provides an overview of Network Address Translation (NAT) and instructions for modifying the default configuration on your HM210dp/di.

8.1 Overview of NAT

Network Address Translation is a method for disguising the private IP addresses you use on your LAN as the public IP address you use on the Internet. You define NAT rules that specify exactly how and when to translate between public and private IP addresses.

In a typical NAT setup, your ISP provides you with a single public IP address to use for your entire network. Then, you assign each computer on your LAN a unique private IP address. (Or, you define a pool of private IP addresses for dynamic assignment to your computers as described in chapter 7 “Configuring DHCP”.

On the HM210dp/di, you set up a NAT rule to specify that whenever one of your computers communicates with the Internet, (that is, it sends and receives IP data packets) its private IP address – which is referenced in each packet – will be replaced by the LAN’s public IP address.

When this type of NAT rule is applied, because the source IP address is swapped out, it appears to other Internet computers as if the data packets are actually originating from the computer assigned your public IP address (in this case, the HM210dp/di).

The NAT rule could further be defined to disguise the source port in the data packet (i.e. change it to another number), so that outside computers will not be able to determine the actual port from which the packet originated. Data packets that arrive in response contain the public IP address as the destination IP address and the disguised source port number. The HM210dp/di changes the IP address and source port number back to the original values (having kept track of the changes it made earlier), and then routes the packet to the originating computer.

NAT rules such as these provide several benefits:

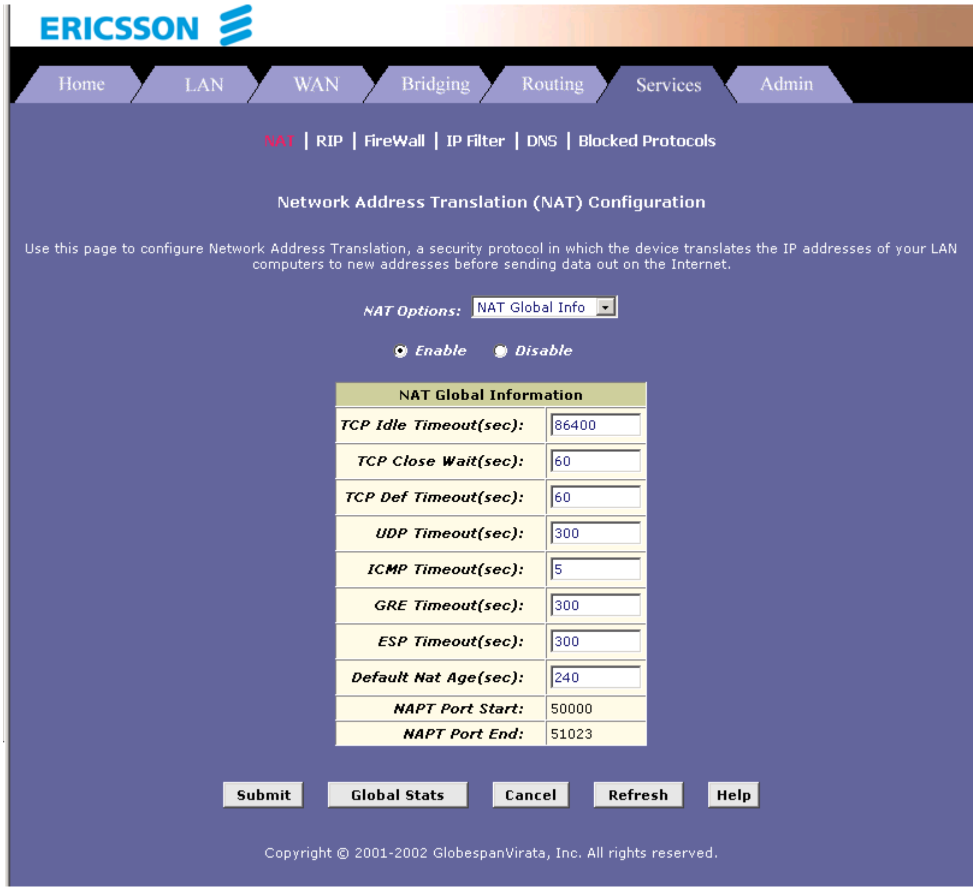
- ❑ They eliminate the need for purchasing multiple public IP addresses for computers on your LAN. You can make up your own private IP addresses at no cost, and then have them translated to the public IP address when your computers access the Internet.

- They provide a measure of security for your LAN by enabling you to assign private IP addresses and then have these and the source port numbers swapped out before your computers access the Internet.

The type of NAT function described above is called *network address port translation (NAPT).* You can use other types, called *flavors,* of NAT for other purposes; for example, providing outside access to your LAN or translating multiple private addresses to multiple public addresses. Section 0 “Adding NAT rules” gives a description of each of the flavors.

8.2 Viewing NAT Configuration

To view your NAT settings, select **Services > NAT**. The **NAT Configuration** page appears:



Network Address Translation (NAT) Configuration

Use this page to configure Network Address Translation, a security protocol in which the device translates the IP addresses of your LAN computers to new addresses before sending data out on the Internet.

NAT Options: NAT Global Info

● *Enable* ○ *Disable*

NAT Global Information	
TCP Idle Timeout(sec):	86400
TCP Close Wait(sec):	60
TCP Def Timeout(sec):	60
UDP Timeout(sec):	300
ICMP Timeout(sec):	5
GRE Timeout(sec):	300
ESP Timeout(sec):	300
Default Nat Age(sec):	240
NAPT Port Start:	50000
NAPT Port End:	51023

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

The **NAT Configuration** page contains the following elements:

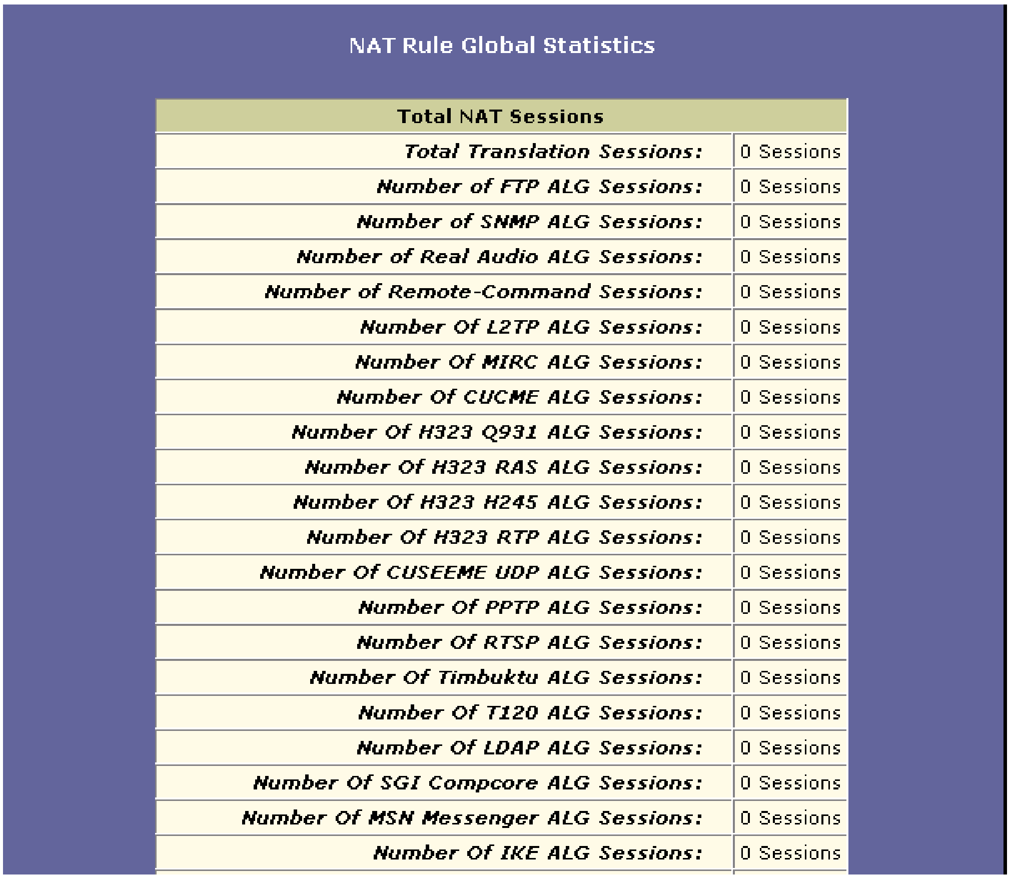
- The *“NAT Options”* drop-down list, which provides access to the NAT Configuration page and Global Information table (shown by default), the NAT Rule Configuration page, and the NAT Translations page.

- Enable/Disable radio buttons, which allow you to turn on or off the NAT feature.
- The NAT Global Information table, which displays the following settings that apply to all NAT rule translations:

Field	Description
TCP Idle Timeout(sec):	When a NAT rule is in effect on a TCP session in the active state, the session will timeout if no packets are received for the specified time.
TCP Close Wait(sec):	When in the TCP session’s closing state, the session will timeout if no packets are received for the specified time.
TCP Def Timeout(sec):	When in the TCP Session’s establishing state, the session will timeout if no packets are received for the specified time.
UDP Timeout(sec):	Same as TCP Idle Timeout, but for UDP packets.
ICMP Timeout(sec):	Same as TCP Idle Timeout, but for ICMP packets.
GRE Timeout(sec):	Same as TCP Idle Timeout, but for GRE packets.
Default NAT Age(sec):	For all other NAT translation sessions, the number of seconds after which a translation session will no longer be valid.
NAPT Port Start/End:	When a NAPT rule is defined, the source ports will be translated to sequential numbers in this range.

If you change any values, click the **Submit** button and then commit your changes to permanent system memory.

You can click the **Global Stats** button to view accumulated data on how many NAT rules have been invoked and how much data has been translated. A page similar to the one below is displayed:



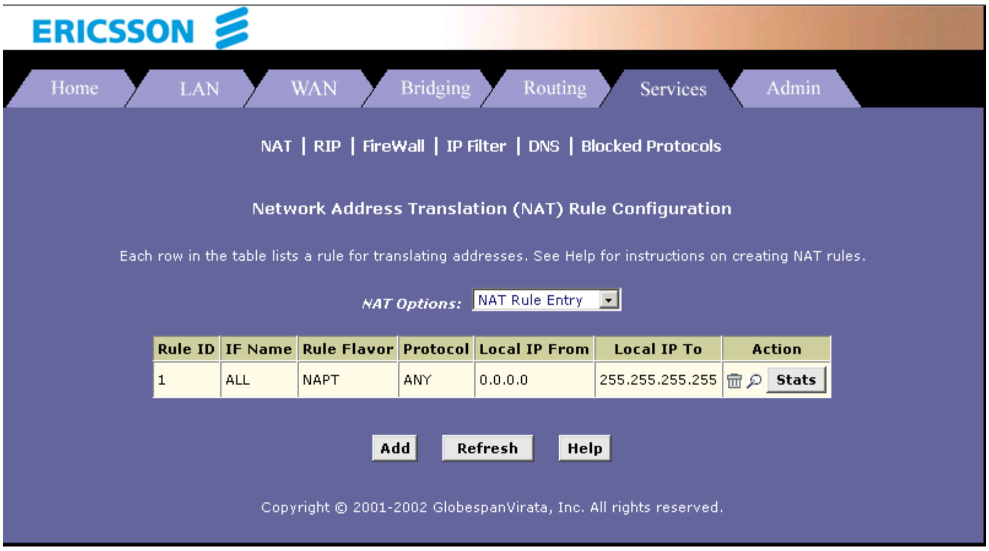
NAT Rule Global Statistics

Total NAT Sessions	
Total Translation Sessions:	0 Sessions
Number of FTP ALG Sessions:	0 Sessions
Number of SNMP ALG Sessions:	0 Sessions
Number of Real Audio ALG Sessions:	0 Sessions
Number of Remote-Command Sessions:	0 Sessions
Number Of L2TP ALG Sessions:	0 Sessions
Number Of MIRC ALG Sessions:	0 Sessions
Number Of CUCME ALG Sessions:	0 Sessions
Number Of H323 Q931 ALG Sessions:	0 Sessions
Number Of H323 RAS ALG Sessions:	0 Sessions
Number Of H323 H245 ALG Sessions:	0 Sessions
Number Of H323 RTP ALG Sessions:	0 Sessions
Number Of CUSEEME UDP ALG Sessions:	0 Sessions
Number Of PPTP ALG Sessions:	0 Sessions
Number Of RTSP ALG Sessions:	0 Sessions
Number Of Timbuktu ALG Sessions:	0 Sessions
Number Of T120 ALG Sessions:	0 Sessions
Number Of LDAP ALG Sessions:	0 Sessions
Number Of SGI Compcore ALG Sessions:	0 Sessions
Number Of MSN Messenger ALG Sessions:	0 Sessions
Number Of IKE ALG Sessions:	0 Sessions

The table provides basic information for each NAT rule you have set up. You can click the **Clear** button to restart the accumulation of the statistics at their initial values.

8.3 Viewing NAT Rules and Rule Statistics

To view the NAT Rules currently defined on your system, select **Services > NAT** and select **NAT Rule Entry** in the NAT Options drop-down list. The **NAT Rule Configuration** page appears:



Network Address Translation (NAT) Rule Configuration

Each row in the table lists a rule for translating addresses. See Help for instructions on creating NAT rules.

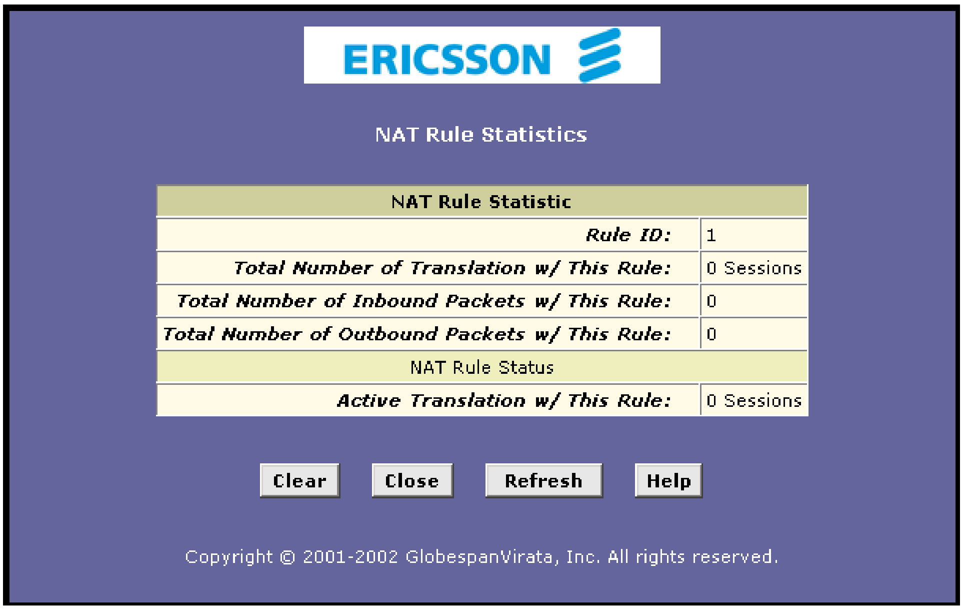
NAT Options: NAT Rule Entry

Rule ID	IF Name	Rule Flavor	Protocol	Local IP From	Local IP To	Action
1	ALL	NAPT	ANY	0.0.0.0	255.255.255.255	🗑 🔍 Stats

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

The NAT Rule Configuration table displays a row containing basic information for each rule. For a description of these fields, refer to the instructions for adding rules in section 0 “Adding NAT Rules”.

From the **NAT Rule Configuration** page, you can click the **Add** button to add a new rule, or use the icons in the “Action” column to delete (🗑) or view details on (🔍) a rule. To view data on how often a specific NAT rule has been used, click **Stats** in the “Action” column. A page similar to the one below appears:



NAT Rule Statistics

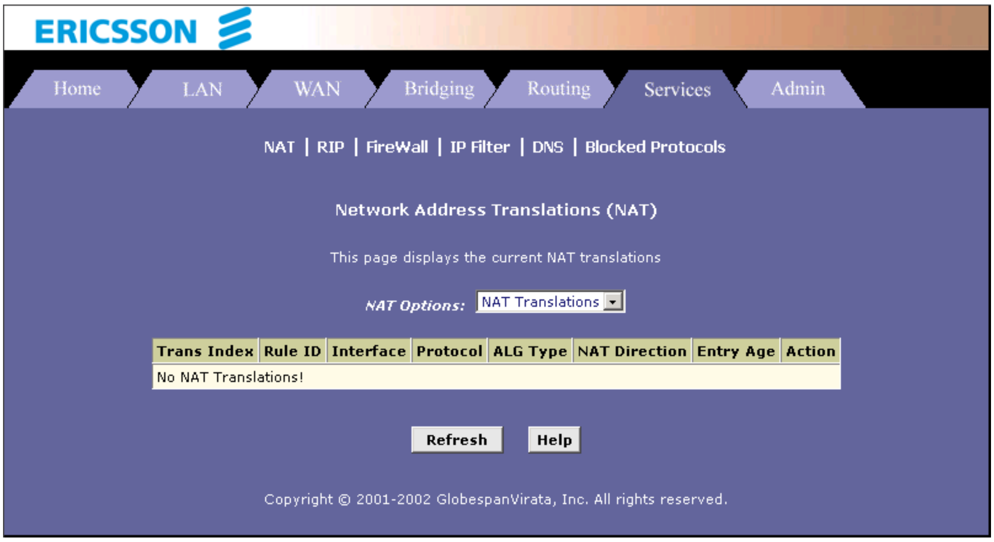
NAT Rule Statistic	
Rule ID:	1
Total Number of Translation w/ This Rule:	0 Sessions
Total Number of Inbound Packets w/ This Rule:	0
Total Number of Outbound Packets w/ This Rule:	0
NAT Rule Status	
Active Translation w/ This Rule:	0 Sessions

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

The statistics show how many times this rule has been invoked and how many currently active sessions are using this rule. You can click the **Clear** button to reset the statistics to zeros and the **Refresh** button to display newly accumulated data.

8.4 Viewing Current NAT Translations

To view a list of NAT translations that have recently been performed and which remain in effect (for any of the defined rules), select **Services > NAT** and select **NAT Translations** in the *NAT Options* drop-down list The **NAT Translations** page appears:



Network Address Translations (NAT)

This page displays the current NAT translations

NAT Options: NAT Translations

Trans Index	Rule ID	Interface	Protocol	ALG Type	NAT Direction	Entry Age	Action
No NAT Translations!							

For each current NAT translation session, the table contains the following fields:

Field	Description
Trans Index	The sequential number assigned to the IP session used by this NAT translation session.
Rule ID	The ID of the NAT rule invoked.
Interface	The device interface on which the NAT rule was invoked (from the rule definition).
Protocol	The IP protocol used by the data packets that are undergoing translations (from the rule definition). Example: TCP, UDP, ICMP.
Alg Type	The *Application Level Gateway (ALG)*, if any, that was used to enable this NAT translation. (ALGs are special settings that certain applications require in

	order to work while NAT is enabled).
NAT Direction	The direction (incoming or outgoing) of the translation (from the port definition). A NAT direction is assigned to each port; the Ethernet port are defined as incoming port, and the WAN ports are defined as outgoing ports. The NAT direction is determined by the interface on which the rule is invoked.
Entry Age	The elapsed time, in seconds, of the NAT translation session.

You can click 🔎 in the “Action” column to view additional details about a NAT translation session. The **NAT Translation – Details** table is displayed. In addition to the information displayed in the NAT Translations table, this table displays the following for the selected current translation sessions:

Field	**Description**
Translated InAddress:	The public IP address to which the private IP address was translated.
In Address:	The private IP address that was translated.
Out Address:	The IP address of the outside destination (web, ftp, site, etc.)
In/Out Pckets:	The number of incoming and outgoing IP packets that have been translated in this translation session.
In Ports:	The actual port number corresponding to the LAN computer.
Out Ports:	The port number associated with the destination address.
Translated In Ports:	The port number to which the LAN computer’s actual port number was translated.

8.5 Adding NAT Rules

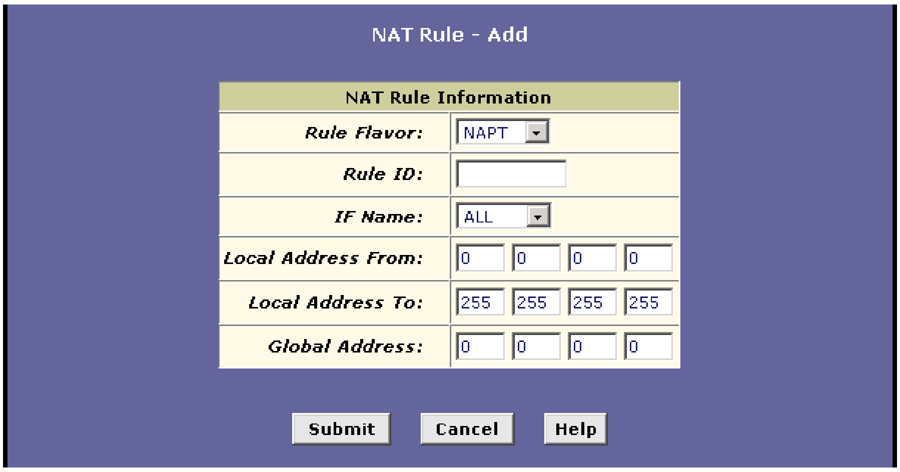
This section explains how to create rules for the various NAT flavors.

8.5.1 The NAPT Rule

The NAT flavor NAPT was used in your default configuration. The NAPT flavor translates all LAN-side private source IP addresses to a single public IP address. It also translates the source port numbers to port numbers that are defined on the **NAT Global Configuration** page.

To create a NAPT rule, proceed as follows:

1. Select **Services > NAT > NAT Rule Entry > Add**. The **NAT Rule – Add** page appears:



NAT Rule - Add

NAT Rule Information				
Rule Flavor:	NAPT			
Rule ID:				
IF Name:	ALL			
Local Address From:	0	0	0	0
Local Address To:	255	255	255	255
Global Address:	0	0	0	0

2. In the *”**Rule Flavor**:”* dropdown list, select **NAPT**.

3. In the *“**Rule ID**:”* field, enter an ID for the rule.
The Rule ID determines the order in which the rules are invoked (the lowest numbered rule is invoked first, and so on). In some case, two or more rules may be fined to act on the same set of IP addresses. Once a data packet matches a rule, the data is acted upon according to that rule and is not subjected to higher-numbered rules.

4. From the *“**IF Name**:”* dropdown list, select the interface on the HM210dp/di to which this rule applies.
Typically, NAT rules apply to communication between your LAN and the Internet. Because the device uses the WAN interface (named ppp-0 or eoa-0) to connect your LAN to your ISP, it is the usual IF Name selection.

5. In the *“**Local Address From/To**:”* fields, type the starting and ending IP addresses respectively, of the range of private IP addresses you want to be translated. Or type the same address in both fields to specify a single IP address.
   If all LAN IP addresses should be translated, specify 0.0.0.0 and 255.255.255.255 respectively.

6. In the *“**Global Address**:”* field, type the address that you want to serve as the publicly known IP address for the LAN computer.

7. When you have completed entering all information, click the **Submit** button. A page appears to confirm the changes.

8. Click **Close** to return to the **NAT Configuration** page. The new rule should no be displayed in the NAT Rule table.

9. On the **NAT Configuration** page, ensure that the **Enable** radio button is selected and then click the **Submit** button. A page appears to confirm your changes.

10. Select **Admin > Commit & Reboot** and click the **Commit** button to save your changes to permanent storage.

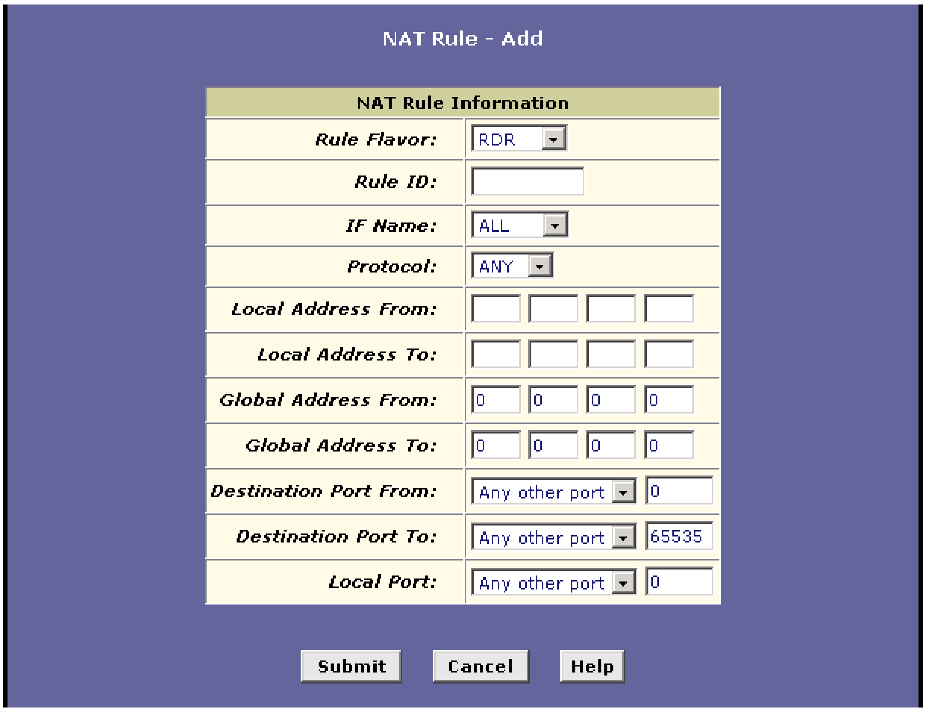
8.5.2 The RDR Rule

You can create a RDR rule to make a computer on your LAN, such as Web or FTP server, available to Internet users without requiring you to obtain a public IP address for that computer. The computer’s private IP address is translated to your public IP address for all incoming and outgoing data packets.

NOTE! Without an RDR rule (or BIMAP rule), the HM210dp/di blocks attempts by external computers to access your LAN computers.

To create a RDR rule, proceed as follows:

1. Select **Services > NAT > NAT Rule Entry > Add**. The **NAT Rule – Add** page appears:



NAT Rule - Add

NAT Rule Information	
Rule Flavor:	RDR
Rule ID:	
IF Name:	ALL
Protocol:	ANY
Local Address From:	. . .
Local Address To:	. . .
Global Address From:	0 . 0 . 0 . 0
Global Address To:	0 . 0 . 0 . 0
Destination Port From:	Any other port 0
Destination Port To:	Any other port 65535
Local Port:	Any other port 0

2. In the *”**Rule Flavor**:”* dropdown list, select **RDR**.

3. In the *“**Rule ID**:”* field, enter an ID for the rule.
   The Rule ID determines the order in which the rules are invoked (the lowest numbered rule is invoked first, and so on). In some case, two or more rules may be fined to act on the same set of IP addresses. Once a data packet matches a rule, the data is acted upon according to that rule and is not subjected to higher-numbered rules.

4. From the *“**IF Name**:”* dropdown list, select the interface on the HM210dp/di to which this rule applies.
   Typically, NAT rules apply to communication between your LAN and the Internet. Because the device uses the WAN interface (named ppp-0 or eoa-0) to connect your LAN to your ISP, it is the usual IF Name selection.

5. Select a *“**Protocol**:”* to which this rule applies, or select **ALL** if the rule applies to all data.

6. In the *“**Local Address From/To**:”* fields, type the same private IP address, or the lowest and highest IP addresses in a range:
   If you type the same IP address in both fields, incoming traffic that matches the criteria of this rule will be redirected to that IP address. If you type a range of IP addresses, incoming traffic will be redirected to any available computer in that range. This option

would typically be used for load balancing, whereby traffic is distributed among several redundant servers.

7. In the *“**Global Address From/To**:”* fields, type the public IP address assigned to you by your ISP.
   If you have multiple WAN interfaces, in both fields type the IP address of the interface to which this rule applies. This rule will not be enforced for data that arrives on WAN interfaces not specified here.
   If you have multiple WAN interfaces and want the rule to be enforced on a range of them, type the starting and ending IP addresses of the range.

8. Enter a destination port ID (or a range) as criteria for incoming traffic.
   Enter a starting and ending port number in the *“**Destination Port From/To**:”* fields if incoming traffic destined for these port types should be redirected to the address(es) specified in step 6. Or, enter the same address in both fields.

9. If the publicly accessible LAN computer uses a non-standard port number for the type of traffic it receives, type the non-standard port number in the *“**Local Port**:”* field.

10. When you have completed entering all information, click the **Submit** button. A page appears to confirm the changes.

11. Click **Close** to return to the **NAT Configuration** page. The new rule should no be displayed in the NAT Rule table.

12. On the **NAT Configuration** page, ensure that the **Enable** radio button is selected and then click the **Submit** button. A page appears to confirm your changes.

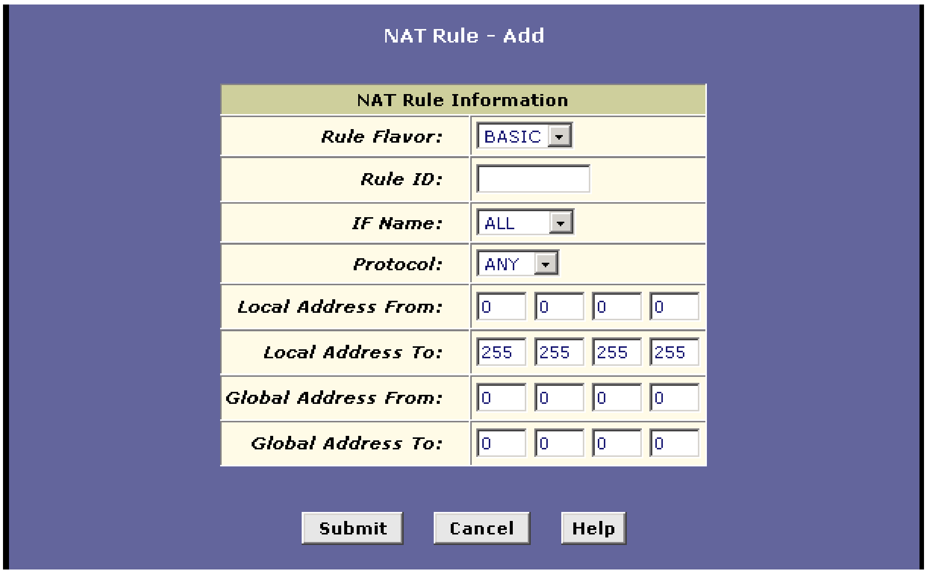
13. Select **Admin > Commit & Reboot** and click the **Commit** button to save your changes to permanent storage.

8.5.3 The BASIC Rule

The BASIC flavor translates the private (LAN-side) IP address to a public (WAN-side) IP address, like the NAPT rule. However, unlike the NAPT rule, the BASIC rule does not translate the port number in the packet header; they are passed through untranslated. Therefore, the BASIC rule does not provide the same level of security as the NAPT rule.

To create a RDR rule, proceed as follows:

1. Select **Services > NAT > NAT Rule Entry > Add**. The **NAT Rule – Add** page appears:



NAT Rule - Add

NAT Rule Information	
Rule Flavor:	BASIC
Rule ID:	
IF Name:	ALL
Protocol:	ANY
Local Address From:	0 0 0 0
Local Address To:	255 255 255 255
Global Address From:	0 0 0 0
Global Address To:	0 0 0 0

2. In the *”**Rule Flavor**:”* dropdown list, select **BASIC**.

3. In the *“**Rule ID**:”* field, enter an ID for the rule.
   The Rule ID determines the order in which the rules are invoked (the lowest numbered rule is invoked first, and so on). In some case, two or more rules may be fined to act on the same set of IP addresses. Once a data packet matches a rule, the data is acted upon according to that rule and is not subjected to higher-numbered rules.

4. From the *“**IF Name**:”* dropdown list, select the interface on the HM210dp/di to which this rule applies.
   Typically, NAT rules apply to communication between your LAN and the Internet. Because the device uses the WAN interface (named ppp-0 or eoa-0) to connect your LAN to your ISP, it is the usual IF Name selection.

5. Select a *“**Protocol**:”* to which this rule applies, or select **ALL** if the rule applies to all data.

6. In the *“**Local Address From/To**:”* fields, type the starting and ending IP addresses that identify the range of private addresses you want to be translated. Or, type the same IP address in both fields.
   If you specify a range, each address will be translated in sequence to a corresponding address in a range of global addresses (which you specify in the next step).

7. In the *“**Global Address From/To**:”* fields, type the starting and ending IP address that identify the pool of public IP addresses to be translated to your private IP addresses. Or, type the same IP address in both fields (if you also specified a single address in the previous step).

8. When you have completed entering all information, click the **Submit** button. A page appears to confirm the changes.

9. Click **Close** to return to the **NAT Configuration** page. The new rule should no be displayed in the NAT Rule table.

10. On the **NAT Configuration** page, ensure that the **Enable** radio button is selected and then click the **Submit** button. A page appears to confirm your changes.

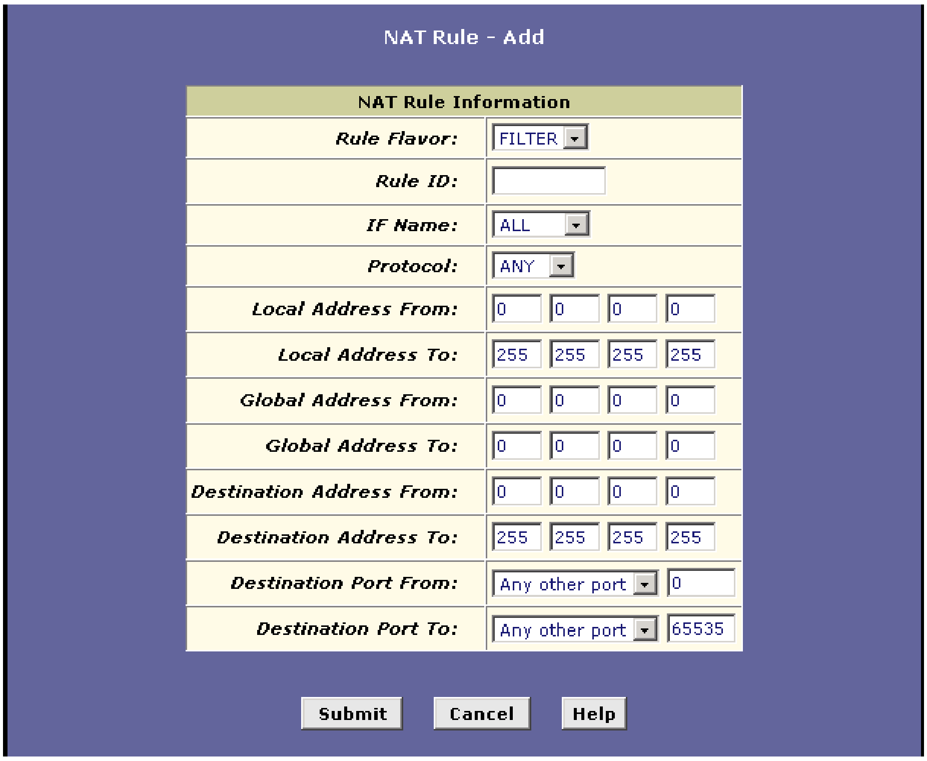
11. Select **Admin > Commit & Reboot** and click the **Commit** button to save your changes to permanent storage.

8.5.4 The FILTER Rule

Like the BASIC flavor, the FILTER flavor translates public and private IP addresses on a one-to-one basis. The FILTER flavor extends the capability of the BASIC rule.
You can use the FILTER rule if you want an address translation to occur only when your LAN computers initiate access to specific destinations. The destinations can be identified by their IP addresses, ser type (such as FTP or Web server), or both.

To create a FILTER rule, proceed as follows:

1. Select **Services > NAT > NAT Rule Entry > Add**. The **NAT Rule – Add** page appears:



NAT Rule - Add

NAT Rule Information

Rule Flavor:	FILTER
Rule ID:	
IF Name:	ALL
Protocol:	ANY
Local Address From:	0 0 0 0
Local Address To:	255 255 255 255
Global Address From:	0 0 0 0
Global Address To:	0 0 0 0
Destination Address From:	0 0 0 0
Destination Address To:	255 255 255 255
Destination Port From:	Any other port 0
Destination Port To:	Any other port 65535

2. In the *”**Rule Flavor**:”* dropdown list, select **FILTER**.

3. In the *“**Rule ID**:”* field, enter an ID for the rule.
   The Rule ID determines the order in which the rules are invoked (the lowest numbered rule is invoked first, and so on). In some case, two or more rules may be fined to act on the same set of IP addresses. Once a data packet matches a rule, the data is acted upon according to that rule and is not subjected to higher-numbered rules.

4. From the *“**IF Name**:”* dropdown list, select the interface on the HM210dp/di to which this rule applies.
   Typically, NAT rules apply to communication between your LAN and the Internet. Because the device uses the WAN interface (named ppp-0 or eoa-0) to connect your LAN to your ISP, it is the usual IF Name selection.

5. Select a *“**Protocol**:”* to which this rule applies, or select **ALL** if the rule applies to all data.

6. In the *“**Local Address From/To**:”* fields, type the starting and ending IP addresses that identify the range of private addresses you want to be translated. Or, type the same IP address in both fields. If you specify a range, each address will be translated in sequence

to a corresponding address in a range of global addresses (which you specify in the next step).

7. In the *“**Global Address From/To**:”* fields, type the starting and ending IP address that identify the pool of public IP addresses to be translated to your private IP addresses. Or, type the same IP address in both fields (if you also specified a single address in the previous step).

8. Enter a *“**Destination Address From/To**:”* ….

9. Enter a starting and ending port number in the *“**Destination Port From/To**:”* fields if incoming traffic destined for these port types should be redirected to the address(es) ….

10. When you have completed entering all information, click the **Submit** button. A page appears to confirm the changes.

11. Click **Close** to return to the **NAT Configuration** page. The new rule should no be displayed in the NAT Rule table.

12. On the **NAT Configuration** page, ensure that the **Enable** radio button is selected and then click the **Submit** button. A page appears to confirm your changes.

13. Select **Admin > Commit & Reboot** and click the **Commit** button to save your changes to permanent storage.

8.5.5 The BIMAP Rule

Unlike the other NAT flavors, the BIMAP flavor performs address translation in both the outgoing and incoming directions.

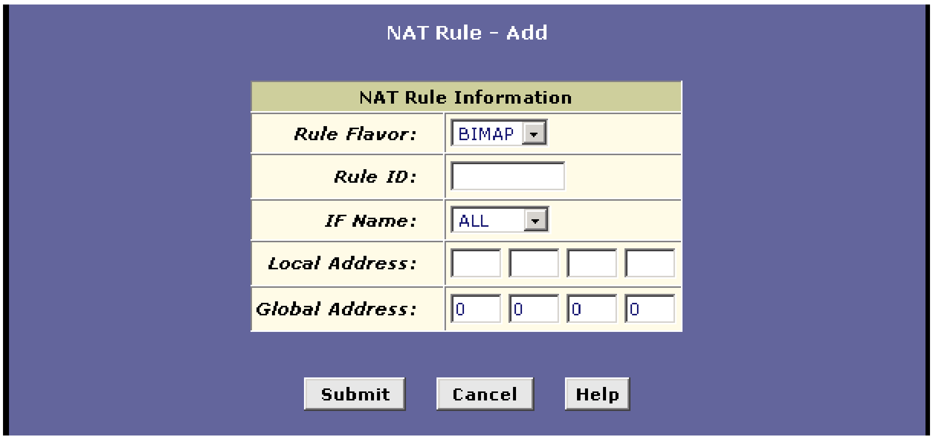
In the incoming direction, when the specified interface receives a packet destined to your public IP address, this address is translated to the private IP address of a computer on your LAN.

In the outgoing direction, the private source IP address in a data packet is translated to the LAN’s public IP address.

BIMAP rules can be used to provide external access to a LAN device. They do not provide the same level of security as RDR rules, because RDR rules also reroute incoming packets based on the port ID. BIMAP rules do not account for the port number, and therefore allow external access regardless of the destination port type specified in the incoming packet.

To create a BIMAP rule, proceed as follows:

1. Select **Services > NAT > NAT Rule Entry > Add**. The **NAT Rule – Add** page appears:



NAT Rule - Add

NAT Rule Information

Rule Flavor:	BIMAP
Rule ID:	
IF Name:	ALL
Local Address:	
Global Address:	0 0 0 0

2. In the *”**Rule Flavor**:”* dropdown list, select **NAPT**.

3. In the *“**Rule ID**:”* field, enter an ID for the rule.
   The Rule ID determines the order in which the rules are invoked (the lowest numbered rule is invoked first, and so on). In some case, two or more rules may be fined to act on the same set of IP addresses. Once a data packet matches a rule, the data is acted upon according to that rule and is not subjected to higher-numbered rules.

4. From the *“**IF Name**:”* dropdown list, select the interface on the HM210dp/di to which this rule applies.
   Typically, NAT rules apply to communication between your LAN and the Internet. Because the device uses the WAN interface (named ppp-0 or eoa-0) to connect your LAN to your ISP, it is the usual IF Name selection.

5. In the *“**Local Address**:”* field, type the private IP address of the computer to which you are granting external access.

6. In the *“**Global Address**:”* field, type the address that you want to serve as the publicly known IP address for the LAN computer.

7. When you have completed entering all information, click the **Submit** button. A page appears to confirm the changes.

8. Click **Close** to return to the **NAT Configuration** page. The new rule should no be displayed in the NAT Rule table.

9. On the **NAT Configuration** page, ensure that the **Enable** radio button is selected and then click the **Submit** button. A page appears to confirm your changes.

10. Select **Admin > Commit & Reboot** and click the **Commit** button to save your changes to permanent storage.

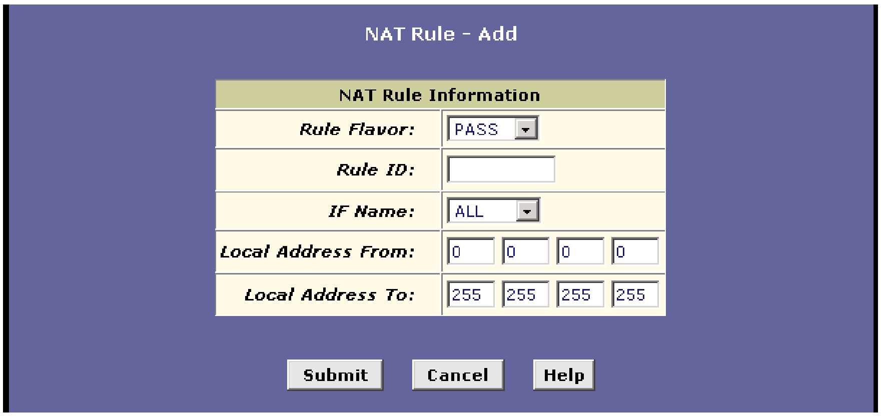
8.5.6 The PASS Rule

You can create a PASS rule to allow a range of IP addresses to remain untranslated when another rule would otherwise do so.

The PASS rule must be assigned a rule ID that is a lower number than the ID assigned to the rule it is intended to pass. If you want a specific IP address or range of addresses to not be subject to an existing rule, say rule ID #5, then you can create a PASS rule with ID #1 through #4.

To create a PASS rule, proceed as follows:

1. Select **Services > NAT > NAT Rule Entry > Add**. The **NAT Rule – Add** page appears:



NAT Rule - Add

NAT Rule Information

Rule Flavor:	PASS
Rule ID:	
IF Name:	ALL
Local Address From:	0 . 0 . 0 . 0
Local Address To:	255 . 255 . 255 . 255

2. In the *"**Rule Flavor**:"* dropdown list, select **PASS**.

3. In the *"**Rule ID**:"* field, enter an ID for the rule.
The Rule ID determines the order in which the rules are invoked (the lowest numbered rule is invoked first, and so on). In some case, two or more rules may be fined to act on the same set of IP addresses. Once a data packet matches a rule, the data is acted upon according to that rule and is not subjected to higher-numbered rules.

4. From the *"**IF Name**:"* dropdown list, select the interface on the HM210dp/di to which this rule applies.
Typically, NAT rules apply to communication between your LAN and the Internet. Because the device uses the WAN interface (named ppp-0 or eoa-0) to connect your LAN to your ISP, it is the usual IF Name selection.

5. In the *“**Local Address From/To**:”* fields, type the lowest and highest IP addresses that define the range of private addresses you want to be passed without translation.
   If you want the PASS rule to act on only one address, type that address in both fields.

6. When you have completed entering all information, click the **Submit** button. A page appears to confirm the changes.

7. Click **Close** to return to the **NAT Configuration** page. The new rule should no be displayed in the NAT Rule table.

8. On the **NAT Configuration** page, ensure that the **Enable** radio button is selected and then click the **Submit** button. A page appears to confirm your changes.

9. Select **Admin > Commit & Reboot** and click the **Commit** button to save your changes to permanent storage.

9 Configuring DNS Server Addresses

Domain Name System (DNS) servers map the user-friendly domain names that users type into their Web browsers (e.g. “yahoo.com”) to the equivalent numerical IP addresses that are used for Internet routing.

When a PC user types a domain name into a browser, the PC must first send a request to a DNS server to obtain the equivalent IP address. The DNS server will attempt to look up the domain name in its own database, and will communicate with higher-level DNS servers when the name cannot be found locally. When the address is found, it is sent back to the requesting PC and is referenced in IP packets for the remainder of the communication.

9.1 Assigning DNS Addresses

Multiple DNS addresses are useful to provide alternatives when one of the servers is down or is encountering heavy traffic. ISPs typically provide primary and secondary DNS addresses, and may provide additional addresses. Your LAN PCs learn these DNS addresses in one of the following ways:

- **Statically;**
  If your ISP provides you with their DNS server addresses, you can assign them to each PC by modifying the PCs IP properties.

- **Dynamically from a DHCP pool;**
  You can configure the DHCP Server feature on the HM210dp/di router and create an address pool that specifies the DNS addresses to be distributed to the PCs. Refer to section 7.3 “Configuring DHCP Server” for instructions on creating DHCP address pools.

In either case, you can specify the actual addresses of the ISP’s DNS servers (on the PC or in the DHCP pool), or you can specify the address of the LAN port on the HM210dp/di (e.g. 192.168.1.1). When you specify the LAN port IP address, the device performs *DNS Relay,* as described in the following section.

Follow the procedures below to connect related devices.

NOTE! If you specify the actual DNS addresses on the PCs or in the DHCP pool, the DNS Relay feature is not used.

9.2 Overview of DNS Relay

When you specify the HM210dp/di's LAN port IP address as the DNS address, then the device automatically performs "DNS relay"; i.e. because the device itself is not a DNS server, it forwards domain name lookup requests it receives from the LAN PCs to a DNS server at the ISP. It then relays the DNS server's response to the PC.

When performing DNS relay, the HM210dp/di must maintain the IP addresses of the DNS servers it contacts. It can learn these addresses in either or both of the following ways:

- **Learned through PPP**;
  If the device uses a PPP connection to the ISP, the primary and secondary DNS addresses can be learned via the PPP protocol. To use this method, the "Use DNS" checkbox must be selected in the PPP interface properties.
  Using this option provides the advantage that you will not need to reconfigure the PCs or the HM210dp/di if the ISP changes their DNS addresses.

- **Configured on the HM210dp/di;**
  You can use the device's DNS feature to specify the ISP's DNS addresses. If the device also uses a PPP interface with the "Use DNS" property enabled, then these configured addresses will be used in addition to the two addresses learned through PPP. If "Use DNS" is not enabled, or if a protocol other than PPP is used (such as EoA), then these configured addresses will be used as the primary and secondary DNS addresses.

9.3 Configuring DNS Relay

Follow these steps to configure DNS Relay:

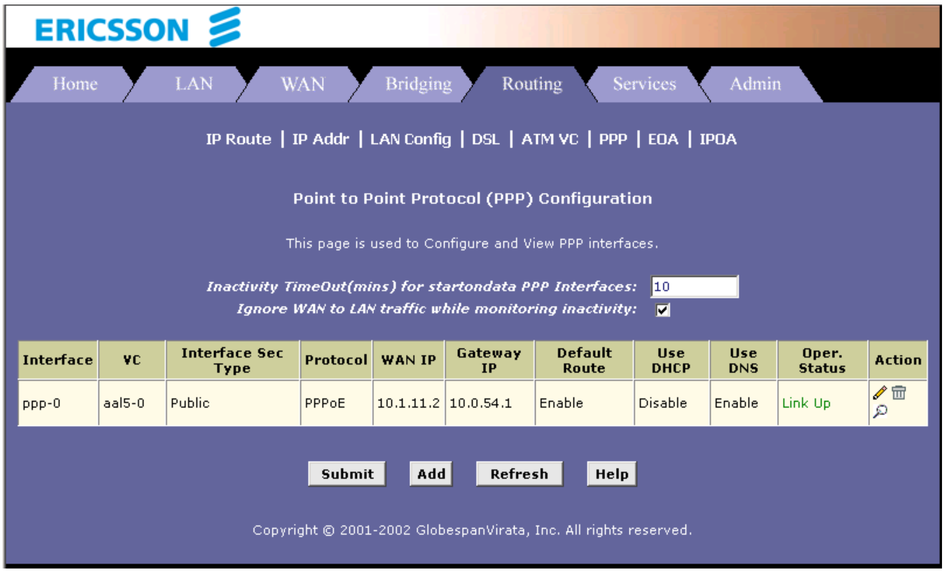
1. Configure the LAN PCs as DHCP clients of the HM210dp/di.

2. Go to **LAN > DHCP Server**, enter the LAN IP address (e.g. **192.168.1.1**) or **0.0.0.0** as the DNS address in the DHCP server pool.
   By default, 0.0.0.0 is already set as the DNS of the DHCP pool.

3. Determine how the HM210dp/di will learn the DNS server address:

   Option 1 – Using a PPP connection to learn the DNS

   Use DNS must be enabled in the PPP interface properties. Go to **Routing > PPP** and check the PPP interface details:



Point to Point Protocol (PPP) Configuration

This page is used to Configure and View PPP interfaces.

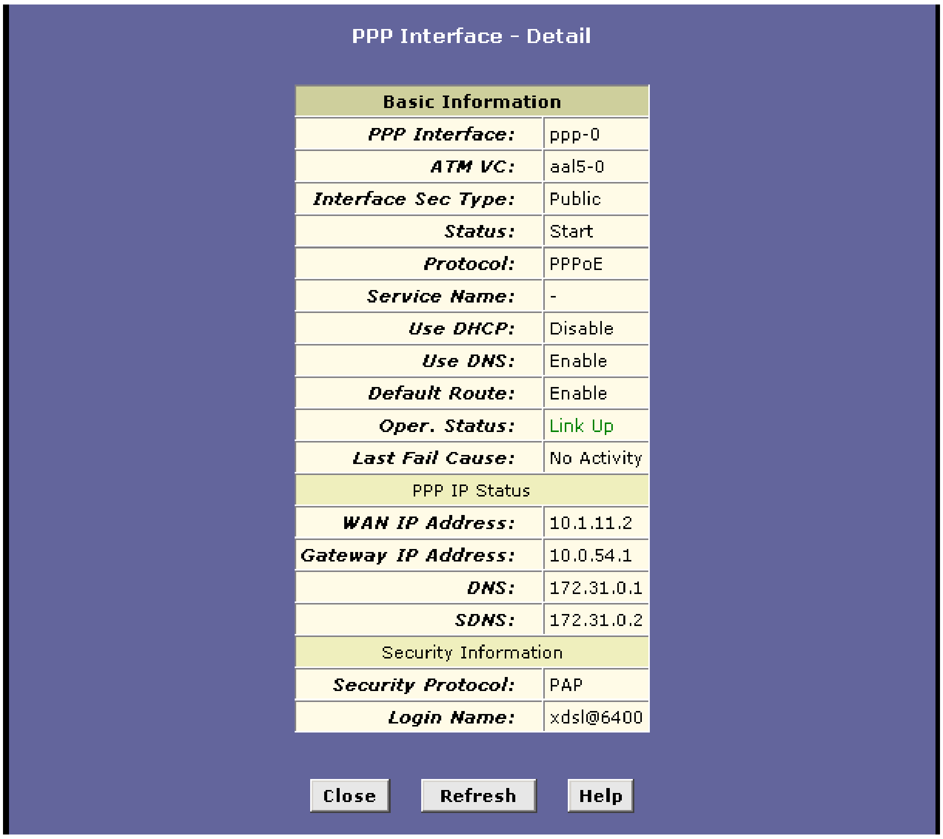
Inactivity TimeOut(mins) for startondata PPP Interfaces: 10

Ignore WAN to LAN traffic while monitoring inactivity: ☑

Interface	VC	Interface Sec Type	Protocol	WAN IP	Gateway IP	Default Route	Use DHCP	Use DNS	Oper. Status	Action
ppp-0	aal5-0	Public	PPPoE	10.1.11.2	10.0.54.1	Enable	Disable	Enable	Link Up	✎ 🗑 🔍

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

If “Use DNS” is disabled, you must delete the interface and create a new one with the new setting.



PPP Interface - Detail

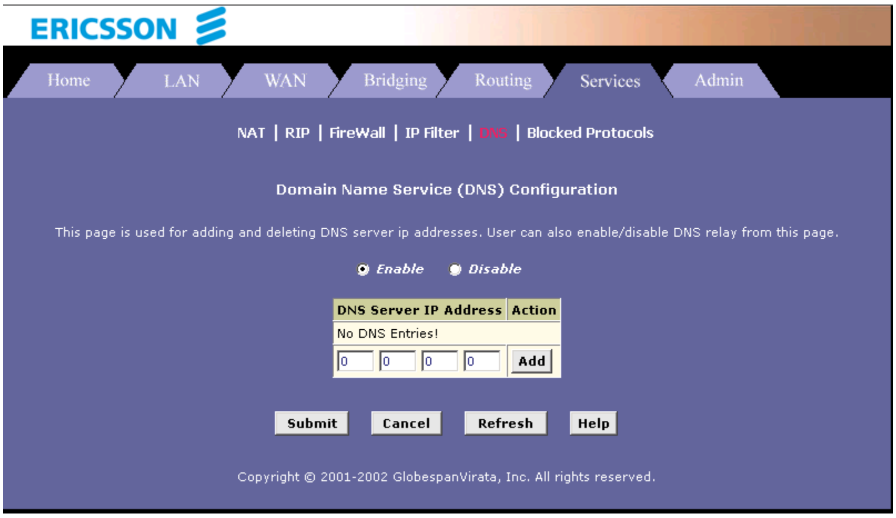
Basic Information	
PPP Interface:	ppp-0
ATM VC:	aal5-0
Interface Sec Type:	Public
Status:	Start
Protocol:	PPPoE
Service Name:	-
Use DHCP:	Disable
Use DNS:	Enable
Default Route:	Enable
Oper. Status:	Link Up
Last Fail Cause:	No Activity
PPP IP Status	
WAN IP Address:	10.1.11.2
Gateway IP Address:	10.0.54.1
DNS:	172.31.0.1
SDNS:	172.31.0.2
Security Information	
Security Protocol:	PAP
Login Name:	xdsl@6400

Option 2 – Configuring DNS on the HM210dp/di:

You can configure the DNS server address to be relayed on the modem if one of the following circumstances applies:

- Not using PPP connection to the ISP (or a protocol other than PPP is used, such as EoA).
- You use PPP connection and “Use DNS” is already Enabled. Then these configured addresses will be used in addition to those DNS addresses learned through PPP.
- You use PPP connection and “Use DNS” is Disabled. Then these configured addresses will be used.

Go to **Service > DNS** to display the **DNS Configuration** page:



Domain Name Service (DNS) Configuration

This page is used for adding and deleting DNS server ip addresses. User can also enable/disable DNS relay from this page.

● Enable ○ Disable

DNS Server IP Address	Action
No DNS Entries!	
0 . 0 . 0 . 0	Add

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Type the IP address of the DNS server in an empty row and click **Add**. Click the *“**Enable**”* radio button, and then click the **Sumbit** button.

Select **Admin > Commit & Reboot** and click the **Commit** button to save your changes to permanent storage.

10 Configuring RIP

The HM210dp/di can be configured to communicate with other routing devices to determine the best path for sending data to its intended destination. This chapter describes how to configure your HM210dp/di to use one of these, called the Routing Information Protocol (RIP).

10.1 Overview of RIP

RIP is an Internet protocol you can set up to share routing table information with other routing devices on your LAN, at your ISP's location, or on remote networks connected to your network via the ADSL line. Generally, RIP is used to enable communication on *autonomous* networks. An autonomous network is one in which all of the computers are administered by the same entity. An autonomous network may be a single network, or a grouping of several networks under the same administration. An example of an autonomous network is a corporate LAN, including devices that can access it from remote locations, such as the computers telecommuters use.

Using RIP, each device sends its routing table to its closes neighbor every 30 seconds. The neighboring device in turn passes the information on to its next neighbor and so on until all devices in the autonomous network have the same set of routes.

Most small home or office networks do not need to use RIP; they have only one router, such as the HM210dp/di, and one path to an ISP. In these cases there is no need to share routes, because all Internet data from the network is sent to the same ISP gateway.

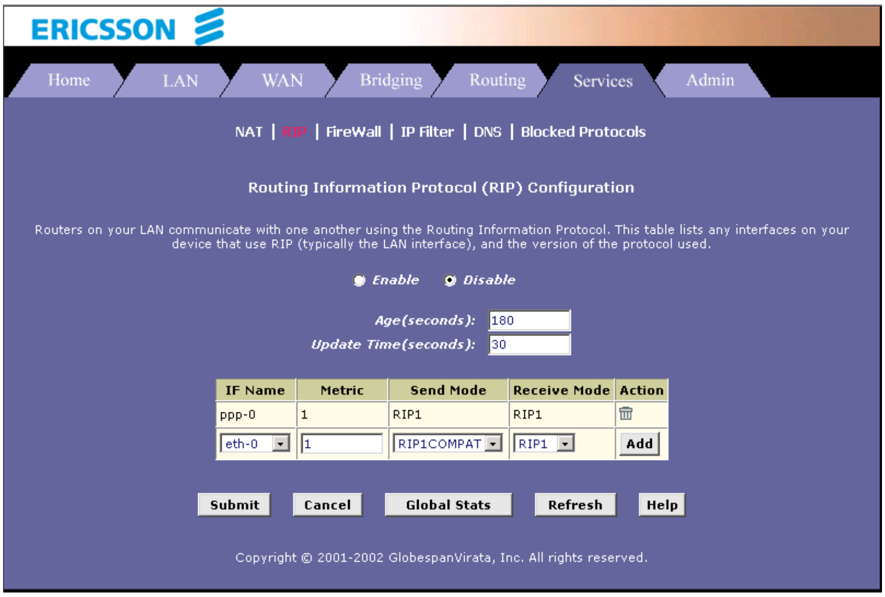
You may want to configure RIP if any of the following circumstances apply to your network:

- Your network includes an additional router or RIP-enabled PC. The HM210dp/di and the router will need to communicate via RIP to share their routing tables.
- Your network connects via the ADSL line to a remote network, such as a corporate network. In order for your LAN to learn the routes used within your corporate network, they should both be configured with RIP.
- Your ISP requests that you run RIP for communication with devices on their network.

10.2 Configuring the RIP

Follow the steps below to configure your HM210dp/di to use RIP:

1. Select **Services > RIP** and the **RIP Configuration** page appears:



Routing Information Protocol (RIP) Configuration

Routers on your LAN communicate with one another using the Routing Information Protocol. This table lists any interfaces on your device that use RIP (typically the LAN interface), and the version of the protocol used.

○ Enable ● Disable

Age(seconds): 180
Update Time(seconds): 30

IF Name	Metric	Send Mode	Receive Mode	Action
ppp-0	1	RIP1	RIP1	🗑
eth-0	1	RIP1COMPAT	RIP1	Add

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

2. The page contains radio buttons for enabling or disabling the RIP feature and a table listing interfaces on which the protocol is currently running. The first time you open this page, the table may be empty.

3. If necessary, change the *“**Age(seconds)**”* and *“**Update Time(seconds)**:”* values. These are global settings for all interfaces that use RIP.

   Age time is the amount of time in seconds that the device’s RIP table will retain each route that it learns from adjacent computers.

   Update Time specifies how frequently the HM210dp/di will send out its routing table to its neighbors.

4. In the “**IF Name**” column, select the interface on which you want to enable RIP.
   For communication with RIP-enables devices on your LAN, select **eth-0** or the name of the appropriate virtual Ethernet interface.
   For communication with your ISP or a remote LAN, select the corresponding ppp, eoa, or other WAN interface.

5. Select a “Metric” value (hop count) for the interface.
   RIP uses a “hop count” as a way to determine the best path to a

given destination in the network. The hop count is the sum of the metric values assigned to each port through which data is passed before reaching the destination. Among several alternative routes, the one with the lowest hop count is considered the fastest path.
For example, if you assign this port a metric of 1, then RIP will add 1 to the hop count when calculating a route that passes through this port. If you know that communication via this interface is slower than through other interfaces on your network, you can assign it a higher metric value that the others.
You can select any integer from 1 to 15.

6. Select a “Send Mode” and a “Receive Mode” according to the following:

   The **Send Mode** setting indicates the RIP version this interface will use when it sends its route information to other devices.

   The **Receive Mode** setting indicates the RIP version(s) in which information must be passed to the HM210dp/di in order to be accepted into its routing table.

   RIP version 1 is the original RIP protocol. Select **RIP1** if you have devices that communicate with this interface that understand RIP version 1 only.
   RIP version 2 is the preferred selection because it supports (classless” IP addresses (which are used to create subnets) and other features. Select **RIP2** if all other routing devices on the autonomous network support this version of the protocol.

7. Click **Add** in the “Action” column and the new RIP entry will be displayed in the table.

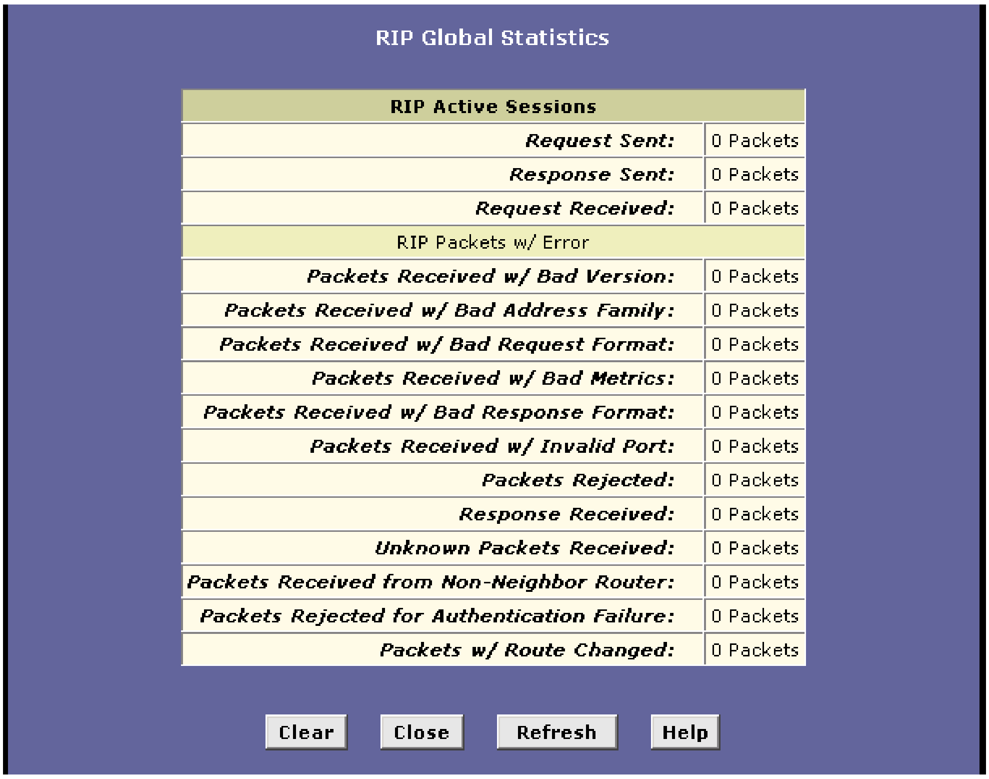
8. Click the *“Enable”* radio button to enable the RIP feature.

9. When you are finished defining RIP interfaces, click the **Submit** button. A page appears to confirm your changes.

10. Select **Admin > Commit & Reboot** and click the **Commit** button to save your changes to permanent storage.

10.3 Viewing RIP Statistics

From the RIP Configuration page, you can click the **Global** Stats button to view statistics on attempts to send and receive route table data over RIP enabled interfaces on the HM210dp/di:



RIP Global Statistics

RIP Active Sessions	
Request Sent:	0 Packets
Response Sent:	0 Packets
Request Received:	0 Packets
RIP Packets w/ Error	
Packets Received w/ Bad Version:	0 Packets
Packets Received w/ Bad Address Family:	0 Packets
Packets Received w/ Bad Request Format:	0 Packets
Packets Received w/ Bad Metrics:	0 Packets
Packets Received w/ Bad Response Format:	0 Packets
Packets Received w/ Invalid Port:	0 Packets
Packets Rejected:	0 Packets
Response Received:	0 Packets
Unknown Packets Received:	0 Packets
Packets Received from Non-Neighbor Router:	0 Packets
Packets Rejected for Authentication Failure:	0 Packets
Packets w/ Route Changed:	0 Packets

You can click the **Clear** button to reset all statistics to zero and the **Refresh** button to display any newly accumulated data.

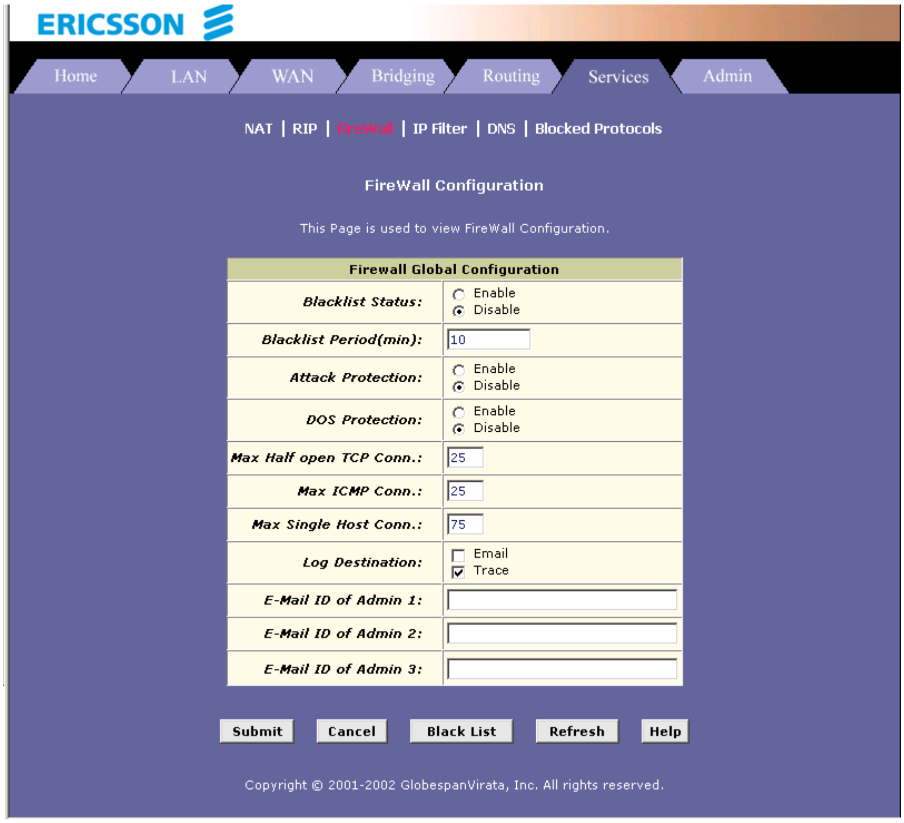
11 Configuring Firewall Settings

The Configuration Manager provides built-in firewall functions, enabling you to protect the system against denial of service (DoS) attacks and other types of malicious accesses to your LAN. You can also specify how to monitor attempted attacks, and who should be automatically notified.

11.1 Global Firewall Settings

Follow the steps below to configure the global firewall settings:

1. Select **Services > Firewall** and the **Firewall Configuration** page appears:



FireWall Configuration

This Page is used to view FireWall Configuration.

Firewall Global Configuration	
Blacklist Status:	○ Enable ● Disable
Blacklist Period(min):	10
Attack Protection:	○ Enable ● Disable
DOS Protection:	○ Enable ● Disable
Max Half open TCP Conn.:	25
Max ICMP Conn.:	25
Max Single Host Conn.:	75
Log Destination:	□ Email ☑ Trace
E-Mail ID of Admin 1:	
E-Mail ID of Admin 2:	
E-Mail ID of Admin 3:	

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

2. Configure the settings according to the following:

Field	Description
Blacklist Status:	If you want the device to maintain and use a black list, click **Enable**. Click **Disable** if you do not want to maintain a list.
Blacklist Period(min):	Specifies the number of minutes that a computer's IP address will remain on the black list.
Attack Protection:	Select **Enable** to use the build-in firewall protections that prevent the following common types of attacks: **IP Spoofing** – Sending packets over the WAN interface using an internal LAN IP address as the source address. **Tear Drop** – Sending packets that contain over-lapping fragments. **Smurf and Fraggle** – Sending packets that use the WAN or LAN IP broadcast address as the source address. **Land Attack** – Sending packets that use the same address as the source and destination address. **Ping of Death** – Illegal IP packets length.
DOS Protection:	Click the **Enable** radio button to use the following denial of service protections: SYN DoS, ICMP DoS and Per-host DoS protection.
Max Half open TCP Conn.:	Sets the percentage of concurrent IP sessions that can be in the half-open state. In ordinary TCP communication, packets are in the half-open state only briefly as a connection is being initiated; the state changes to active when packets are being exchanged, or closed when the exchange is complete. TCP connections in the half-open state can use up the available IP sessions. If the percentage is exceeded, then the half-open sessions will be closed and replaced with new sessions as they are initiated.
Max ICMP Conn.:	Sets the percentage of concurrent IP sessions that can be used for ICMP messages. If the percentage is exceeded, older ICMP IP sessions will be replaced by new sessions as

	they are initiated.
Max Single Host Conn.:	Sets the percentage of concurrent IP sessions that can originate from a single computer. This percentage should take into account the number of hosts on the LAN.
Log Destination:	Specifies how attempted violations of the firewall settings will be tracked. Records of such events can be sent out via Ethernet to be handled by a system utility Ethernet to (Trace) or can be e-mailed to specified administrators.
E-Mail ID of Admin 1/2/3:	Specifies the e-mail address(es) of the administrator(s) who should receive notices of any attempted firewall violations. Type the address(es) in standard internet e-mail address format, e.g. *j.smith@onecompany.xom* The e-mail message will contain the time of the violation, the source address of the computer responsible for the violation, the destination IP address, the protocol being used, the source and destination ports, and the number of violations occurring the previous 30 minutes. If the ICMP protocol were being used, then instead of the source and destination ports, the e-mail will report the ICMP code and type.

3. Click the **Submit** button.

4. Select **Admin > Commit & Reboot** and click the **Commit** button to save your changes to permanent storage.

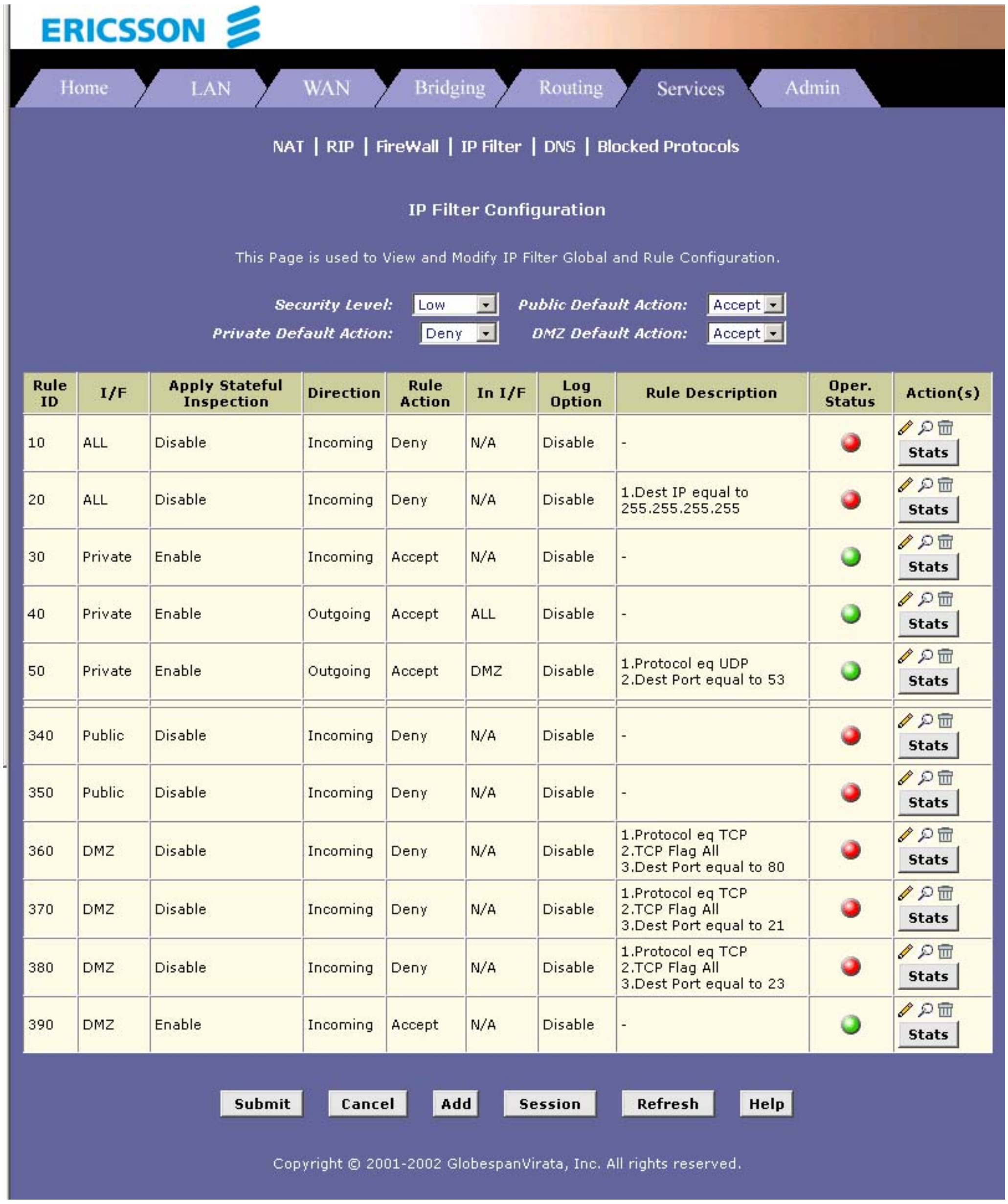
11.2 Configuring IP Filters

When you define an IP filter rule and enable the feature, you instruct the HM210dp/di to examine each data packet it receives to determine whether it meets criteria set forth in the rule. The criteria can include the size of the packet, the network or internet protocol it is carrying, the direction in which it is traveling (for example from the LAN to the Internet or vice versa), the IP address of the sending computer, the destination IP address, and other characteristics of the packet data.

If the packet matches the criteria established in a rule, the packet can either be accepted (forwarded towards its destination) or denied (discarded) depending on the action specified in the rule.

11.2.1 Viewing Your IP Filter Configuration

To view your IP filter configuration, select **Services > IP Filter**. The **IP Filter Configuration** page appears:



IP Filter Configuration

This Page is used to View and Modify IP Filter Global and Rule Configuration.

Security Level: Low *Public Default Action:* Accept

Private Default Action: Deny *DMZ Default Action:* Accept

Rule ID	I/F	Apply Stateful Inspection	Direction	Rule Action	In I/F	Log Option	Rule Description	Oper. Status	Action(s)
10	ALL	Disable	Incoming	Deny	N/A	Disable	-	🔴	✎ 🔍 🗑 Stats
20	ALL	Disable	Incoming	Deny	N/A	Disable	1.Dest IP equal to 255.255.255.255	🔴	✎ 🔍 🗑 Stats
30	Private	Enable	Incoming	Accept	N/A	Disable	-	🟢	✎ 🔍 🗑 Stats
40	Private	Enable	Outgoing	Accept	ALL	Disable	-	🟢	✎ 🔍 🗑 Stats
50	Private	Enable	Outgoing	Accept	DMZ	Disable	1.Protocol eq UDP 2.Dest Port equal to 53	🟢	✎ 🔍 🗑 Stats
340	Public	Disable	Incoming	Deny	N/A	Disable	-	🔴	✎ 🔍 🗑 Stats
350	Public	Disable	Incoming	Deny	N/A	Disable	-	🔴	✎ 🔍 🗑 Stats
360	DMZ	Disable	Incoming	Deny	N/A	Disable	1.Protocol eq TCP 2.TCP Flag All 3.Dest Port equal to 80	🔴	✎ 🔍 🗑 Stats
370	DMZ	Disable	Incoming	Deny	N/A	Disable	1.Protocol eq TCP 2.TCP Flag All 3.Dest Port equal to 21	🔴	✎ 🔍 🗑 Stats
380	DMZ	Disable	Incoming	Deny	N/A	Disable	1.Protocol eq TCP 2.TCP Flag All 3.Dest Port equal to 23	🔴	✎ 🔍 🗑 Stats
390	DMZ	Enable	Incoming	Accept	N/A	Disable	-	🟢	✎ 🔍 🗑 Stats

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

The **IP Filter Configuration** page displays global settings that you can modify, and the IP filter rule table, which shows all currently established rules. When rules are defined, you can use the icons in the “Action(s)” column to edit (✎), delete (🗑) and view details on (🔍) the corresponding rule.

11.2.2 Configuring IP Filter Global Settings

The **IP Filter Configuration** page enables you to configure several global IP Filter settings, and displays a table showing all existing IP Filter rules. The global settings that you can configure are:

- **Security Level**: When **High** is selected, only those rules that are assigned a security value of "High" will be in effect. The same is true for the **Medium** and **Low** settings. When **None** is selected, IP Filtering is disabled.

- **Private/Public/DMZ Default Action**: This setting specifies a default action to be taken (**Accept** or **Deny** on private, public or DMZ-type devise interfaces when they receive packets that **do not** match any of the filtering rules.

  Private – Typically, the global setting for private interfaces is **Accept**, so that LAN computers have access to the Internet connection of the HM210dp/di.

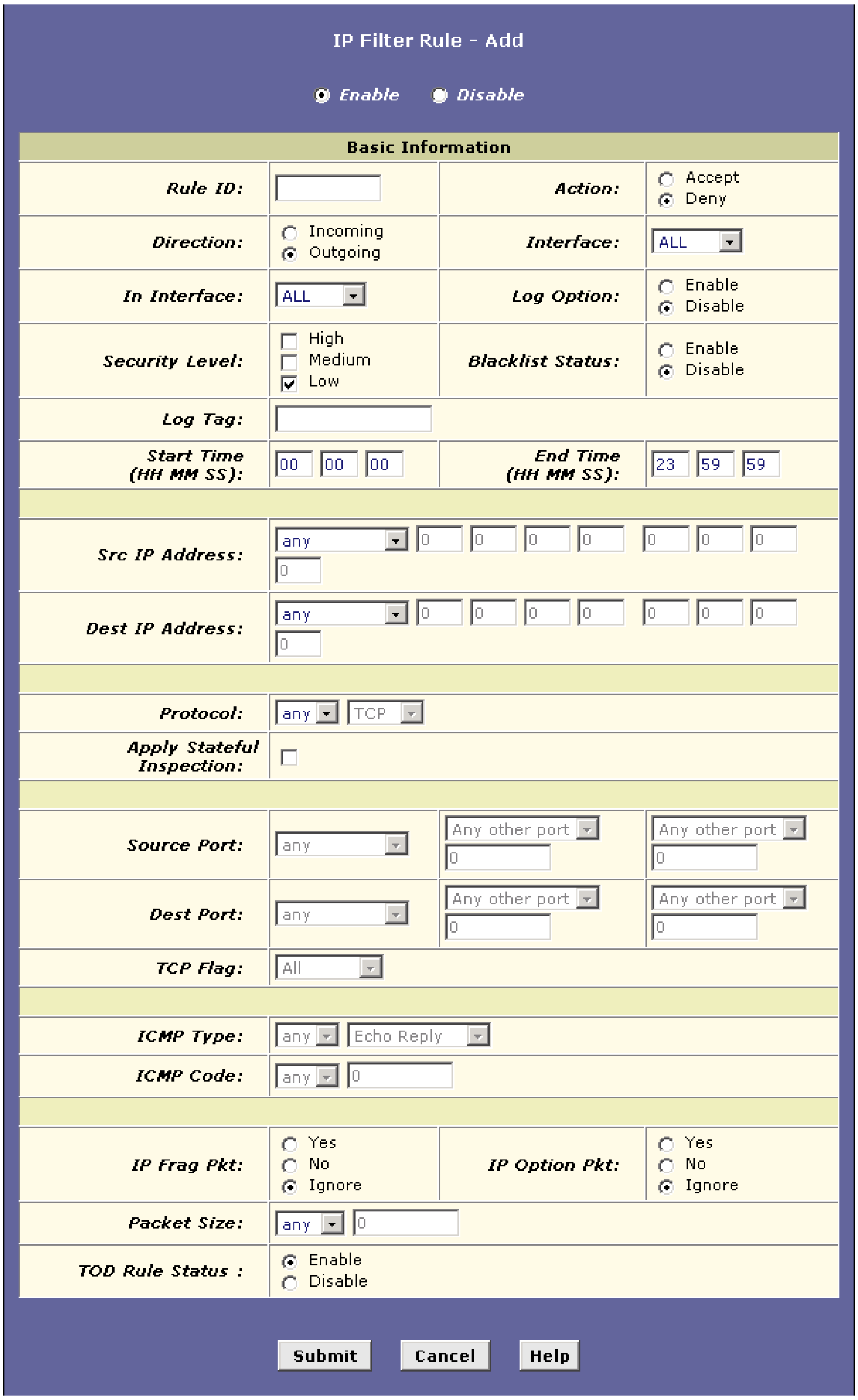
  Public – The interface connect to the Internet, e.g. PPP, EoA and IpoA interfaces. Typically, the global setting for public interfaces is **Deny**, so that all accesses to your LAN initiated from external computers are denied (discarded at the public interface), except for those allowed by a specific IP Filter rule.

  DMZ – Refers to computers that are available for both public and in-network accesses (such as a company's public Web server). Packets received on a DMZ interface – whether from a LAN or external source – are subject to a set of protections that is in between public and private interfaces. The global setting for DMZ-type interfaces may be set to **Deny** so that all attempts to access these servers are denied by default. The administrator may then configure IP Filter rules to allow accesses of certain types.

11.2.3 Creating IP Filter Rules

To create an IP filter rule, you set various criteria that must be met in order for the rule to be invoked. Use these instructions to add a new IP filter rule, and refer to the examples in section 11.2.3.1 for assistance:

1. On the main **IP Filter Configuration** page, click the **Add** button. The **IP Filter Rule – Add** page appears:



IP Filter Rule - Add

● Enable ○ Disable

Basic Information

Rule ID:		Action:	○ Accept ● Deny
Direction:	○ Incoming ● Outgoing	Interface:	ALL ▾
In Interface:	ALL ▾	Log Option:	○ Enable ● Disable
Security Level:	□ High □ Medium ☑ Low	Blacklist Status:	○ Enable ● Disable
Log Tag:			
Start Time (HH MM SS):	00 00 00	End Time (HH MM SS):	23 59 59
Src IP Address:	any ▾ 0 0 0 0 0 0 0 0		
Dest IP Address:	any ▾ 0 0 0 0 0 0 0 0		
Protocol:	any ▾ TCP ▾		
Apply Stateful Inspection:	□		
Source Port:	any ▾	Any other port ▾ 0	Any other port ▾ 0
Dest Port:	any ▾	Any other port ▾ 0	Any other port ▾ 0
TCP Flag:	All ▾		
ICMP Type:	any ▾ Echo Reply ▾		
ICMP Code:	any ▾ 0		
IP Frag Pkt:	○ Yes ○ No ● Ignore	IP Option Pkt:	○ Yes ○ No ● Ignore
Packet Size:	any ▾ 0		
TOD Rule Status :	● Enable ○ Disable		

2. Enter or select data for each field that applies to your rule:

Field	Description
Rule ID:	Rules are processed from lowest to highest on each data packet, until a match is found. It is recommended that you assign rule Ids in multiples of 5 or 10 (e.g. 10, 20, 30) so that you leave enough space between them for inserting a new rule if necessary.
Action:	The action can be **Accept** (forward to destination) or **Deny** (discard the packet).
Direction:	**Incoming** refers to packets coming from the LAN, and **outgoing** refers to packets going to the Internet. You can use rules that specify the incoming direction to restrict external computers from accessing your LAN.
Interface:	The interface on which the rule will take affect.
In Interface:	The interface from which packets must have been forwarded to the interface specified in the previous section. This option is valid only for the outgoing direction.
Log Option:	When **Enable** is selected, a log entry will be created on the system each time this rule is invoked.
Security Level:	The security level that must be enabled globally for this rule to take affect. A rule will be active only if its security level is the same as the globally configured setting (shown on the main IP Filter page). For example, if the rule is set to “Medium” and the global firewall level is set to “Medium”, then the rule w ill be active; but if the global firewall level is set to “High” or “Low”, then the rule will be inactive.
Blacklist Status:	Specifies whether or not a violation of this rule w ill result in the offending computer’s IP address being added to the Black List, which blocks the router from forwarding packets from that source for a specified period of time.
Log Tag:	A description of up to 16 characters to be recorded in the log in the event that a packet violates this rule. Be sure to set the Log Option to

	Enable if you configure a Log Tag.
Start/End Time:	The time range during which this rule is to be in effect, specified in military units.
Src IP Address:	IP address criteria for the source computer(s) from which the packet originates. Use the following expressions to specify IP: **any**: any source IP address **lt**: less than **lteq**: less than or equal to **gt**: greater than **eq**: equal to **neq**: not equal to **range**: within the specified range, inclusive **out of range**: outside the specified range **self**: the IP address of the router interface on which this rule takes effect.
Dest IP Address:	IP address rule criteria for the destination computer(s), i.e. the IP address of the computer to which the packet is being sent. In addition to the options described for the “Src IP Address” field, the following option is available: **bcast**: Specifies that the rule will be invoked for any packets sent to the broadcast address for the receiving interface. (The broadcast address is used to send packets to all hosts on the LAN or subnet connected to the specified interface). When you select this option, you do not need to specify the address, so the address fields are dimmed.
Protocol:	The basic IP protocol criteria that must be met for a rule to be invoked. Using the options in the drop-down list, you can specify that packets must contain the selected protocol (eq), that they must not contain the specified protocol (neq), or that the rule can be invoked regardless of the protocol (any). TCP, UDP and ICMP are commonly IP protocols; others can be identified by number from 0-255 as defined by IANA.
Apply Stateful Inspection:	If this option is enabled, then **stateful filtering** is performed and the rule is also applied in the other direction on the given interface during an IP session.

Source Port:	Port number criteria for the computer(s) from which the packet originates. This field will be dimmed (unavailable for entry) if you have not specified a protocol critera. See the description of Src IP Address for the selection options.
Dest Port:	Port number criteria for the destination computer(s), i.e. the port number of the type of computer to which the packet is being sent. This field will be dimmed (unavailable for entry) unless you have selected TCP or UDP as the protocol. See the description of Src IP Address for the selection options.
TCP Flag:	Specifies whether the rule should apply only to TCP packets that contain the synchronous (SYN) flag, only to those that contain the non-synchronous (NOT-SYN) flag, or to all TCP packets. This field will be dimmed (unavailable for entry) unless you selected TCP as the protocol.
ICMP Type:	Specifies whether the value in the type field in ICMP packet headers will be used as a criteria. The code value can be any decimal value from 0 to 255. You can specify that the value must be equal (eq) or not equal (neq) to the specified value, or you can select any to enable the rule to be invoked on all ICMP packets. This field will be dimmed (unavailable for entry) unless you specify ICMP as the protocol.
ICMP Code:	Specifies whether the value in the code field in ICMP packet headers will be used as criteria. The code value can be any decimal value from 0 to 255. You can specify that the value must be equal (eq) or not equal (neq) to the specified value, or you can select any to enable the rule to be invoked on all ICMP packets. This field will be dimmed (unavailable for entry) unless you specify ICMP as the protocol.
IP Frag Pkt:	Determines how the rule applies to IP packets that contain fragments. You can choose from the following options: **Yes**: The rule will be applied only to packets that contain fragments. **No**: The rule will be applied only to packets that do not contain fragments.

	Ignore: (Default) The rule will be applied to packets whether or not they contain fragments, assuming that they match the other criteria.
IP Option Pkt:	Determines whether the rule should apply to IP packets that have options specified in their packet headers. You can choose from the following options: **Yes**: The rule will be applied only to packets that contain header options. **No**: The rule will be applied only to packets that do not contain header options. **Ignore**: (Default) The rule will be applied to packets whether or not they contain header options, assuming that they match the other criteria.
Packet Size:	Specifies that the IP Filter rule will take affect only on packets whose size in bytes matches this criteria. (lt=less than, gt=greater than, lteq=less than or equal to, etc).
TOD Rule Status:	The Time of Day Rule Status determines how the Start Time/End Time settings are used. **Enable**: (Default) The rule is in effect for the specified time period. **Disable**: The rule is not in effect for the specified time period, but is effective at all other times.

3. When you are done selecting criteria, ensure that the **Enable** radio button is selected and then click the **Submit** button.

   If the security level of the rule matches the globally configured setting, a green ball in the “Status” column for that rule, indicating that the rule is now in effect. A red ball will display when the rule is disabled or if its security level is different than the globally configured level.

4. Ensure that the **Security Level** and **Private/Public/DMZ Default Action** settings on the **IP Filter configuration** page are configured as needed, then click the **Submit** button.

5. Select **Admin > Commit & Reboot** and click the **Commit** button to save your changes to permanent storage.

11.2.3.1 IP Filter Rule Examples

Example 1 – Blocking a specific computer on your LAN from accessing web servers on the Internet;

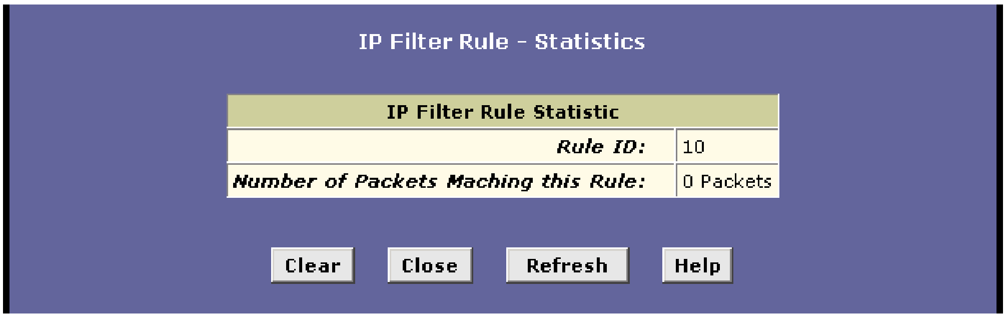
1. Add a new rule for outgoing packets on the ppp-0 interface from any incoming interface (this would include the eth-0 interface, for example).
2. Specify a source IP address of the computer you want to block.
3. Specify the Protocol = TCP and enable the Store State setting.
4. Specify a destination port = 80, which is the standard port number for web servers.
5. Enable the rule by clicking the radio button at the top of the page.
6. Click **Submit** to create the rule.
7. On the **IP Filter Configuration** page, set the **Security Level** to the same level you chose for the rule, and set both the **Private Default Action** and the **Public Default Action** to **Accept**.
8. Click **Submit** to commit your changes.

Example 2 – Blocking Telnet access to the device;

1. Add a new rule for incoming packets on the ppp-0 interface.
2. Specify that the packet must contain the TCP protocol, and must be destined for port 23, the standard port number used for the Telnet protocol.
3. Enable the rule by clicking the radio button at the top of the page.
4. Click **Submit** to create the rule, and commit your changes.

11.2.4 Viewing IP Filter Statistics

To view statistics on how many packets were accepted or denied for a rule, select **Services > IP Filter > Stats** in the row corresponding to the rule. The **IP Filter Rule – Statistics** page displays:



IP Filter Rule - Statistics

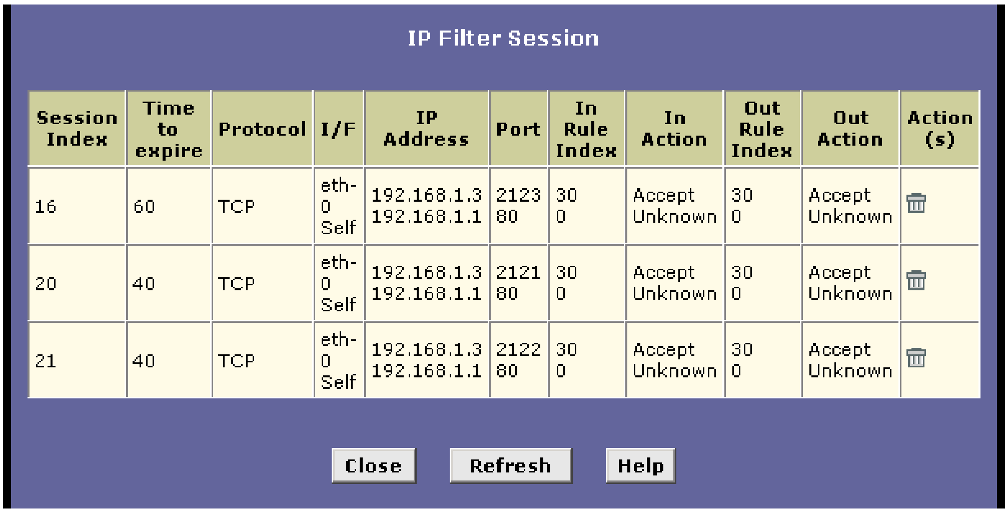
IP Filter Rule Statistic	
Rule ID:	10
Number of Packets Maching this Rule:	0 Packets

You can click the **Clear** button to reset the count to zero and the **Refresh** button to display newly accumulated data.

11.2.5 Managing Current IP Filter Sessions

When two computers communicate using the IP protocol, an IP session is created for the duration of the communication. The HM210dp/di allows a fixed number of concurrent IP sessions. You can view information about each current IP session and delete sessions (for security reasons, for example).

To view all current IP sessions, select **Services > IP Filter > Session** to display the **IP Filters Session** page:



IP Filter Session

Session Index	Time to expire	Protocol	I/F	IP Address	Port	In Rule Index	In Action	Out Rule Index	Out Action	Action (s)
16	60	TCP	eth-0 Self	192.168.1.3 192.168.1.1	2123 80	30 0	Accept Unknown	30 0	Accept Unknown	🗑
20	40	TCP	eth-0 Self	192.168.1.3 192.168.1.1	2121 80	30 0	Accept Unknown	30 0	Accept Unknown	🗑
21	40	TCP	eth-0 Self	192.168.1.3 192.168.1.1	2122 80	30 0	Accept Unknown	30 0	Accept Unknown	🗑

The **IP Filter Session** table displays the following fields for each current IP session:

Field	Description
Session Index	The ID assigned by the system to the IP session (all sessions, whether or not they are affected by an IP

	filter rule, are assigned a session index).
Time to expire	The number of seconds in which the connection will automatically expire.
Protocol	The underlying IP protocol used on the connection, such as TCP, UDP, IGMP, etc.
I/F	The interface on which the IP Filter rule is effective.
IP Address	The IP address involved in the communication. The first one shown is the initiator of the communication.
Port	The hardware addresses of the ports involved in the communication.
In/Out Rule Index	The number of the IP Filter rule that is applied to this session (assigned when the rule was created).
In/Out Action	The action (accept, deny, or unknown) being taken on data coming in to or going out from the interface. This action is specified in the rule definition.
Actions	Provides a icon you can click on (🗑) to delete the IP session. When you delete a session, the communication between is discontinued.

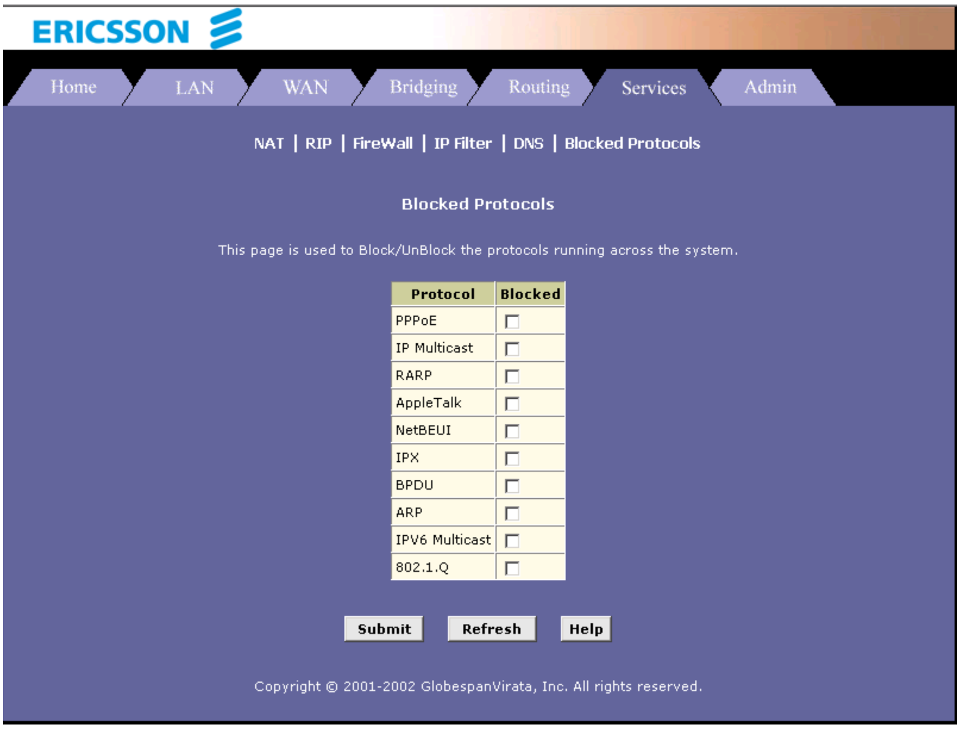
You can click the **Refresh** button to display newly accumulated data.

11.3 Blocking Specific Protocols

The Blocked Protocols feature enables you to prevent the HM210dp/di from passing any data that uses a particular protocol. Unlike the IP Filter feature, you cannot specify additional criteria for blocked protocols, such as particular users or destinations.

NOTE! Blocking certain protocols may disrupt or disable your network communication or Internet access. DO NOT use this feature unless you are certain that a particular protocol is not needed or wanted on your network.

To block specific protocols running across the system, select **Services > Blocked Protocols**. The **Blocked Protocols** page appears:



Blocked Protocols

This page is used to Block/UnBlock the protocols running across the system.

Protocol	Blocked
PPPoE	☐
IP Multicast	☐
RARP	☐
AppleTalk	☐
NetBEUI	☐
IPX	☐
BPDU	☐
ARP	☐
IPV6 Multicast	☐
802.1.Q	☐

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Check the protocol type you want to block and click the **Submit** button. Make sure to use the **Commit** feature to save your changes to the permanent memory.

To unblock a specific protocol, uncheck the protocol and repeat the submit and commit tasks.

The following list describes each of the available protocols:

Protocol	**Description**
PPPoE	Point-to-Point Protocol over Ethernet. Many DSL modems use PPPoE to establish and maintain a connection with a service provider. PPPoE provides a means of logging in to the ISPs servers so that they can authenticate you as a customer and provide you access to the Internet. Check with your ISP before blocking this protocol.
IP Multicast	IP Multicast is an extension to the IP protocol. It enables individual packets to be sent to multiple hosts on the Internet, and is often used for handling e-mail mailing lists and teleconferencing/videoconferencing.
RARP	Reverse Address Resolution Protocol. This IP protocol provides a way for computers to determine their own IP addresses when they only know their

	hardware address (i.e. MAC addresses). Certain types of computers, such as diskless workstations, must use RARP to determine their IP address before communicating with other network devices.
AppleTalk	A networking protocol used for Apple Macintosh networks.
NetBEUI	NetBIOS Enhanced User Interface. On many LAN operating systems, the NetBEUI rotocol provides the method by which computers identify themselves to and communicate with each other.
IPX	Internetwork Packet Exchange. A networking protocol used on Novell Netware-based LANs.
BPDU	Bridge Protocol Data Unit. BPDUs are data messages that are exchanged across the switches between LANs that are connected by a bridge. BPDU packets contain information on ports, addresses, priorities, and costs, and are exchanged across bridges to detect and eliminate loops in a network.
ARP	Address Resolution Protocol. Computers on a LAN use ARP to learn the hardware addresses (i.e. MAC addresses) of other computers when they know only their IP addresses.
IPV6 Multicast	IP Multicasting under IP Protocol version 6. See IP Multicast above.
802.1.Q	This IEEE specification defines a protocol for *virtual LANs* on Ethernet networks. A virtual LAN is a group of PCs that function as a local area network, even though the PCs may not be physically connected. They are commonly used to facilitate administration of large networks.

12 Administration Tasks

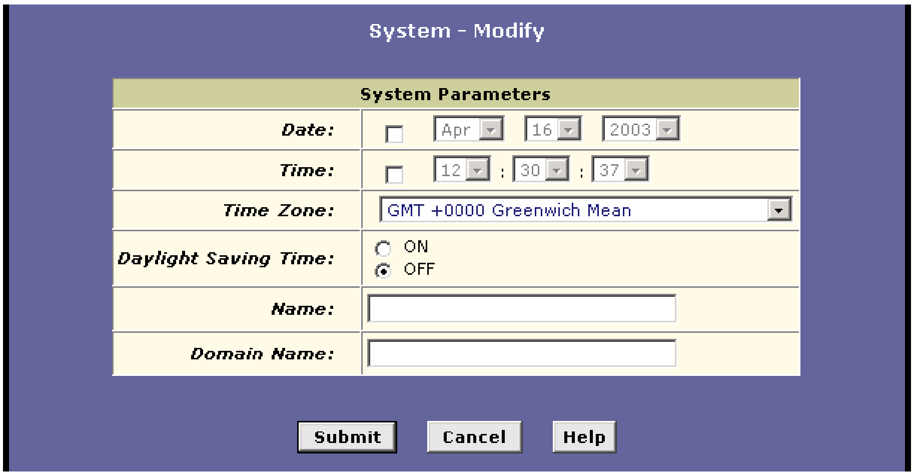
12.1 Changing the System Date and Time

The HM210dp/di keeps a record of the current date and time, which it uses to calculate and report various performance data.

You can change the date and time as required. On this page you may also specify the host name and the domain name in the fields provided.

Follow these instructions to change basic system information:

1. Select **Home > Modify** to display the **System – Modify** page:



System Parameters	
Date:	□ Apr 16 2003
Time:	□ 12 : 30 : 37
Time Zone:	GMT +0000 Greenwich Mean
Daylight Saving Time:	○ ON ● OFF
Name:	
Domain Name:	

2. Modify the fields on this page as required. The following table describes each field:

Field	Description
Date: *Time:*	These fields initially appear dimmed. To modify the date and time, click the respective check boxes and select the appropriate values from the drop-down lists. The time displays in military format.
Time Zone: *Daylight Saving Time:*	You can select your time zone from the drop-down list, and then click the appropriate radio button to indicate whether Daylight Savings Time

	is currently in effect. After you initially set the time, turning DST on or off will adjust the current displayed time by one hour in the appropriate direction. You must remember to change the DST option each spring and fall – it will not change automatically.
Name:	You can use this field to specify an easy-to-remember name for the HM210dp/di. The next time you want to access the Configuration Manager, you can type this name in the location box in your Web browser, instead of typing the numeric IP address. For example, if you entered *myrouter* in this field (and left the Domain Name field blank) then you could type the following in your Web browser to access the Configuration Manager: http://myrouter **(Note!** This will only work if you are using the HM210dp/di's DNS relay feature. This feature is automatically enabled when the DNS server address configured on your PCs is also the address assigned to the LAN port on the HM210dp/di.
Domain Name:	You can use this field to specify and Internet domain name for the HM210dp/di. The next time you access the Configuration Manager, you can type the domain name and the device name (see the Name field above) in your Web browser. For example, if you entered *myrouter* iin the Name field and *mydomain.com* in the Domain Name field, then you would type the following in your Web browser to access the Configuration Manager: http://myrouter.mydomain.com

3. When you are finished modifying the settings, click the **Submit** button.

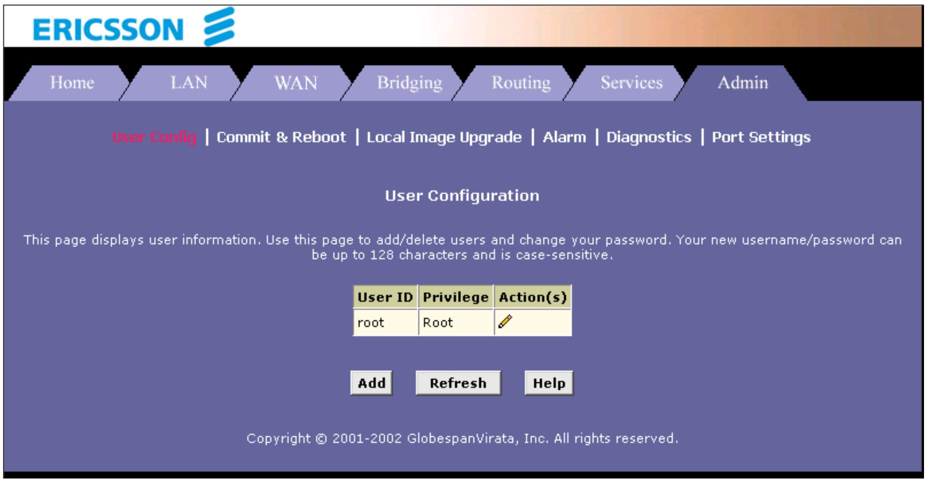
4. Select **Admin > Commit & Reboot** and click the **Commit** button to save your changes to permanent storage.

12.2 Configuring User Names and Passwords

The first time you log into the Configuration Manager, you use the default User ID and Password (root and root). The system allows two levels of privilege: **Root** and **User**. Root privilege allows you to change and commit the device's settings while user privilege is provided with read-only access rights.

To add login User Id or change the login password, proceed as follows:

1. Select **Admin > User Config**. The **User Configuration** page appears:


ERICSSON
Home
LAN
WAN
Bridging
Routing
Services
Admin
User Config | Commit & Reboot | Local Image Upgrade | Alarm | Diagnostics | Port Settings
Add
Refresh
Help

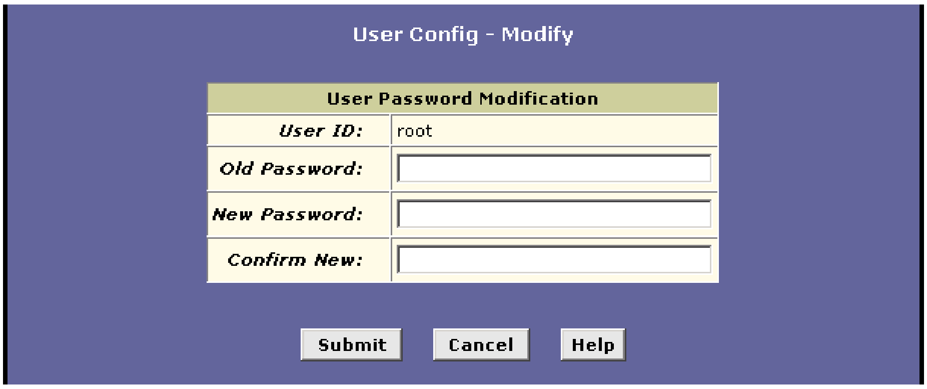
User Configuration

This page displays user information. Use this page to add/delete users and change your password. Your new username/password can be up to 128 characters and is case-sensitive.

User ID	Privilege	Action(s)
root	Root	✎

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

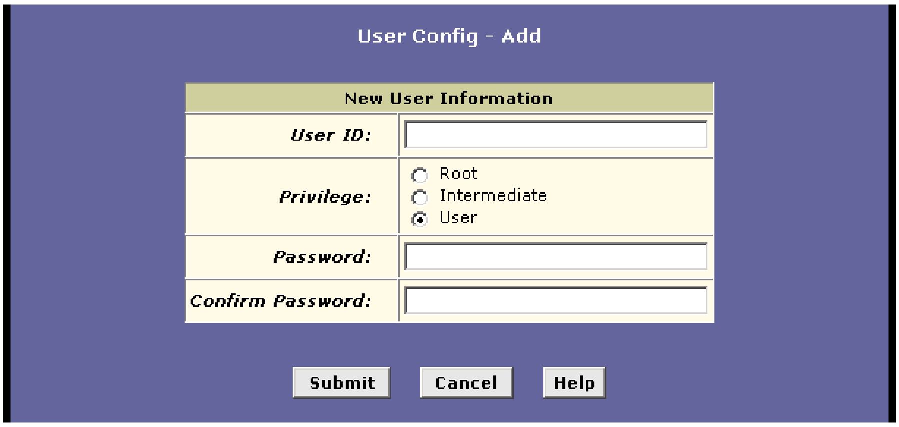
2. To modify the login password click the ✎ (modify) icon in the “Action(s)” column and then change the current password:



User Config - Modify

User Password Modification	
User ID:	root
Old Password:	
New Password:	
Confirm New:	

3. To add a new login ID, click the **Add** button (on the User Configuration page) to display the **User Config – Add** page. Enter your settings in the fields provided.
NOTE! Both the User ID and Password are case sensitive.



User Config - Add

New User Information	
User ID:	
Privilege:	○ Root ○ Intermediate ● User
Password:	
Confirm Password:	

4. After making changes, click the **Submit** button.

5. Select **Admin > Commit & Reboot** and click the **Commit** button to save your changes to permanent storage.

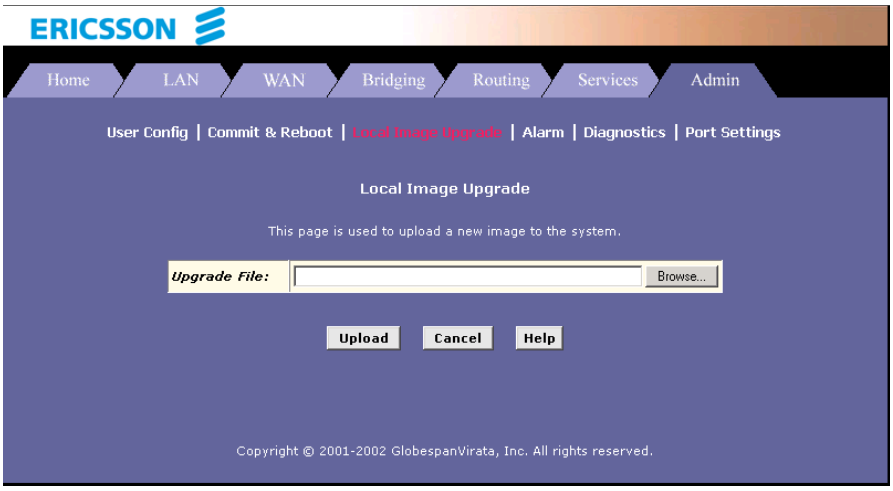
12.3 Upgrading the Software

This option allows you to upgrade the software running on the HM210dp/di. All system software is contained in a single file, called an *image.* The image is composed of several distinct parts, each of which implements a different set of functions.

The Configuration Manager provides an easy way to upload a new software image, or a specific part of the image, to the memory on the HM210dp/di.

To perform the upgrade task, download the required image file to your local host PC and follow the steps below:

1. Select **Admin > Local Image Upgrade** to view the **Local Image Upgrade** page:


ERICSSON
Home
LAN
WAN
Bridging
Routing
Services
Admin
User Config | Commit & Reboot | Local Image Upgrade | Alarm | Diagnostics | Port Settings
Browse...
Upload
Cancel
Help

Local Image Upgrade

This page is used to upload a new image to the system.

Upgrade File:

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

2. Click **Browse** to locate the firmware file. The name of the upgrade file must be one of the following:
   TEImage.bin, TEDsl.gsz, TEAppl.gsz, Filesys.bin, TEPatch.bin.

3. Click the **Upload** button to start the upgrade. After a few seconds, a message like the following should appear (the file name may differ):

```
File: TEDs1.gsz successfully saved to the flash.
Please reboot for the new image to take effect.
```

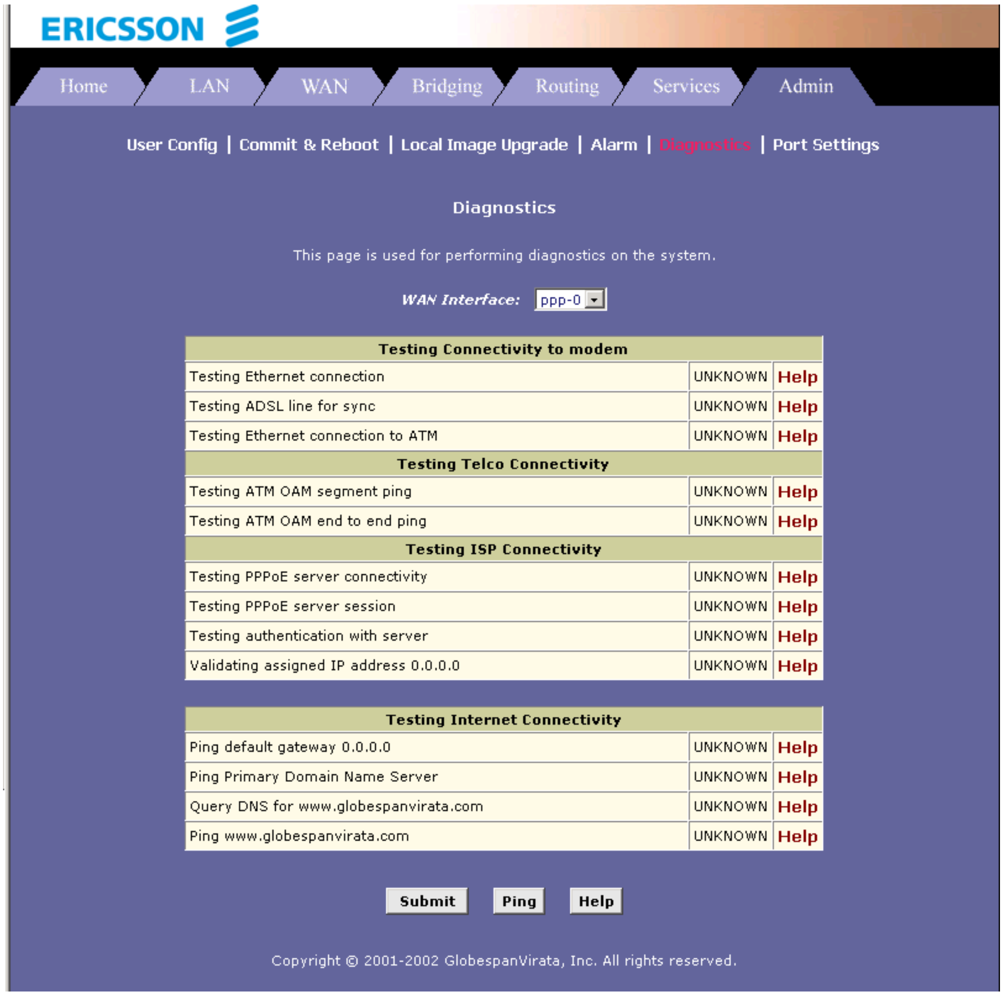
4. Power off the unit, wait a few seconds, and then turn it on again to activate the new software.

NOTE! DO NOT interrupt the upgrade process. Otherwise it might cause damage to your modem.

12.4 Using Diagnostics

The diagnostics feature executes a series of test of your system software and hardware connections. Use this feature when working with your ISP to troubleshoot problems.

To perform diagnostics on ATM VC, select **Admin > Diagnostics**.


ERICSSON
Home
LAN
WAN
Bridging
Routing
Services
Admin
User Config | Commit & Reboot | Local Image Upgrade | Alarm | Diagnostics | Port Settings
Submit
Ping
Help

Diagnostics

This page is used for performing diagnostics on the system.

WAN Interface: ppp-0

Testing Connectivity to modem		
Testing Ethernet connection	UNKNOWN	Help
Testing ADSL line for sync	UNKNOWN	Help
Testing Ethernet connection to ATM	UNKNOWN	Help
Testing Telco Connectivity		
Testing ATM OAM segment ping	UNKNOWN	Help
Testing ATM OAM end to end ping	UNKNOWN	Help
Testing ISP Connectivity		
Testing PPPoE server connectivity	UNKNOWN	Help
Testing PPPoE server session	UNKNOWN	Help
Testing authentication with server	UNKNOWN	Help
Validating assigned IP address 0.0.0.0	UNKNOWN	Help

Testing Internet Connectivity		
Ping default gateway 0.0.0.0	UNKNOWN	Help
Ping Primary Domain Name Server	UNKNOWN	Help
Query DNS for www.globespanvirata.com	UNKNOWN	Help
Ping www.globespanvirata.com	UNKNOWN	Help

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

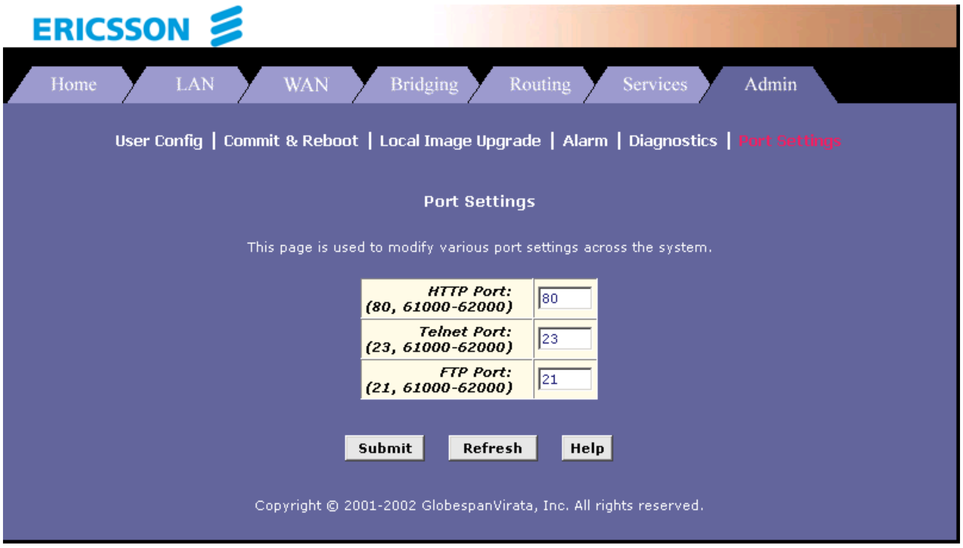
Select the VC on which you want to execute diagnostics and then click the **Submit** button.

The diagnostics utility will run a series of test to check whether the device’s connections are up and working. This takes only a few seconds and the results for each test are displayed on screen. A test may be skipped if the program determines that no suitable interface is configured on which to run the test.

You can click **Help** to display an explanation of each test. Work with your ISP to interpret the results of the diagnostic tests.

12.5 Modifying Port Settings

The modem's HTTP/Telnet/FTP services are accessible using the standard port number 80, 23 and 21 respectively. It is possible that you want to designate a publicly accessible HTTP, Telnet or FTP server on your LAN side and you want to shift the modem's HTTP/Telnet/FTP service to use a non-standard port number. If this is the case, select **Admin > Port Settings** to view the **Port Settings** page:


ERICSSON
Home
LAN
WAN
Bridging
Routing
Services
Admin
User Config | Commit & Reboot | Local Image Upgrade | Alarm | Diagnostics | Port Settings
Submit
Refresh
Help

Port Settings

This page is used to modify various port settings across the system.

HTTP Port: *(80, 61000-62000)*	80
Telnet Port: *(23, 61000-62000)*	23
FTP Port: *(21, 61000-62000)*	21

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Modify the port settings and click the **Submit** button.

Select **Admin > Commit & Reboot** and click the **Commit** button to save your changes to permanent storage.

12.5.1 Accessing a Server with a Non-Standard Port Number

If you set the modem's embedded HTTP/Telnet/FTP server to use a non-standard port number, when access from the external world, the IP address should be followed by a colon and the non-standard port number, as shown in the following example for a HTTP server (i.e. the Web-based Configuration Manager):

```
http://10.0.1.16:61000
```

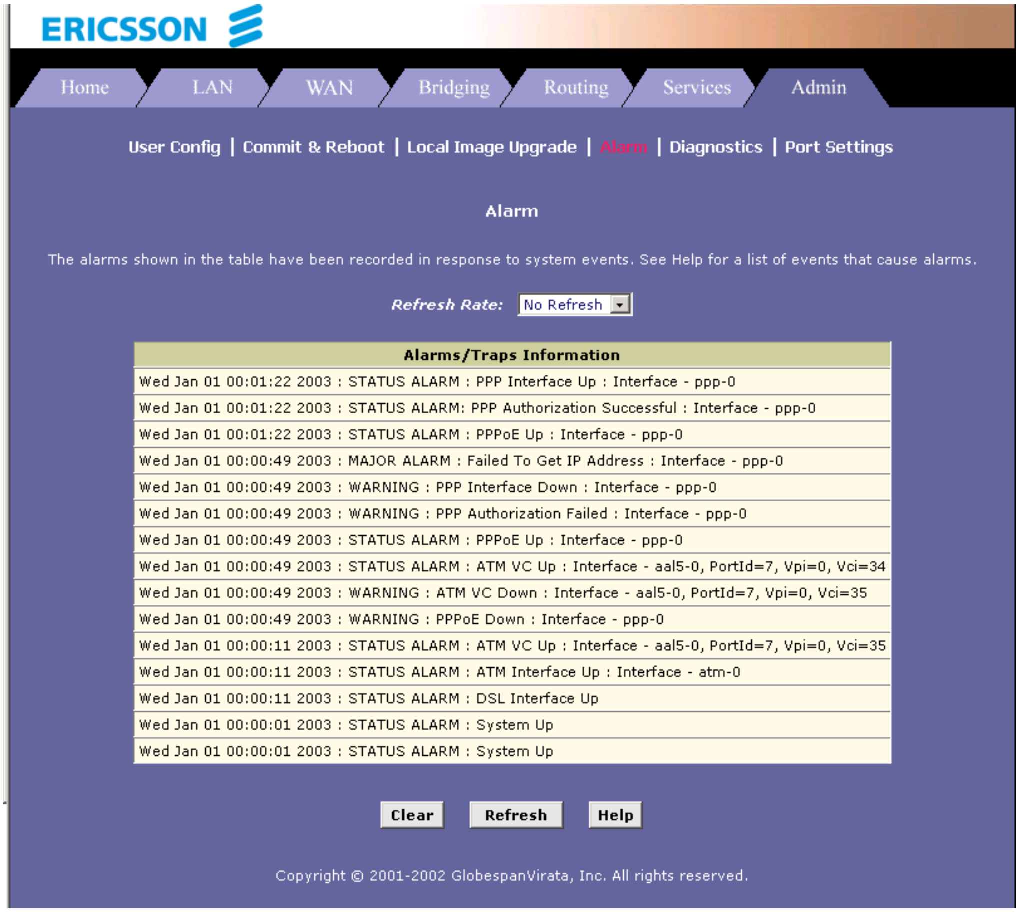
where 10.0.1.16 is the modem's WAN IP address and 61000 is the non-standard port number for HTTP that you specified in the Port Settings page.

12.6 Viewing System Alarms

You can use the Configuration Manager to view information about alarms that occur in the system. Alarms, also called traps, are caused by a variety of system events, including connection attempts, resets, and configuration changes.

Although you will not typically need to view this information, it may be helpful in working with your ISP to troubleshoot problems you encounter with the device. (Despite their name, not all alarms indicate problems in the functioning of the system).

To display the Alarm page, select **Admin > Alarm**:


ERICSSON
Home
LAN
WAN
Bridging
Routing
Services
Admin
User Config | Commit & Reboot | Local Image Upgrade | Alarm | Diagnostics | Port Settings
Clear
Refresh
Help

Alarm

The alarms shown in the table have been recorded in response to system events. See Help for a list of events that cause alarms.

Refresh Rate: No Refresh

```
Alarms/Traps Information
Wed Jan 01 00:01:22 2003 : STATUS ALARM : PPP Interface Up : Interface - ppp-0
Wed Jan 01 00:01:22 2003 : STATUS ALARM: PPP Authorization Successful : Interface - ppp-0
Wed Jan 01 00:01:22 2003 : STATUS ALARM : PPPoE Up : Interface - ppp-0
Wed Jan 01 00:00:49 2003 : MAJOR ALARM : Failed To Get IP Address : Interface - ppp-0
Wed Jan 01 00:00:49 2003 : WARNING : PPP Interface Down : Interface - ppp-0
Wed Jan 01 00:00:49 2003 : WARNING : PPP Authorization Failed : Interface - ppp-0
Wed Jan 01 00:00:49 2003 : STATUS ALARM : PPPoE Up : Interface - ppp-0
Wed Jan 01 00:00:49 2003 : STATUS ALARM : ATM VC Up : Interface - aal5-0, PortId=7, Vpi=0, Vci=34
Wed Jan 01 00:00:49 2003 : WARNING : ATM VC Down : Interface - aal5-0, PortId=7, Vpi=0, Vci=35
Wed Jan 01 00:00:49 2003 : WARNING : PPPoE Down : Interface - ppp-0
Wed Jan 01 00:00:11 2003 : STATUS ALARM : ATM VC Up : Interface - aal5-0, PortId=7, Vpi=0, Vci=35
Wed Jan 01 00:00:11 2003 : STATUS ALARM : ATM Interface Up : Interface - atm-0
Wed Jan 01 00:00:11 2003 : STATUS ALARM : DSL Interface Up
Wed Jan 01 00:00:01 2003 : STATUS ALARM : System Up
Wed Jan 01 00:00:01 2003 : STATUS ALARM : System Up
```

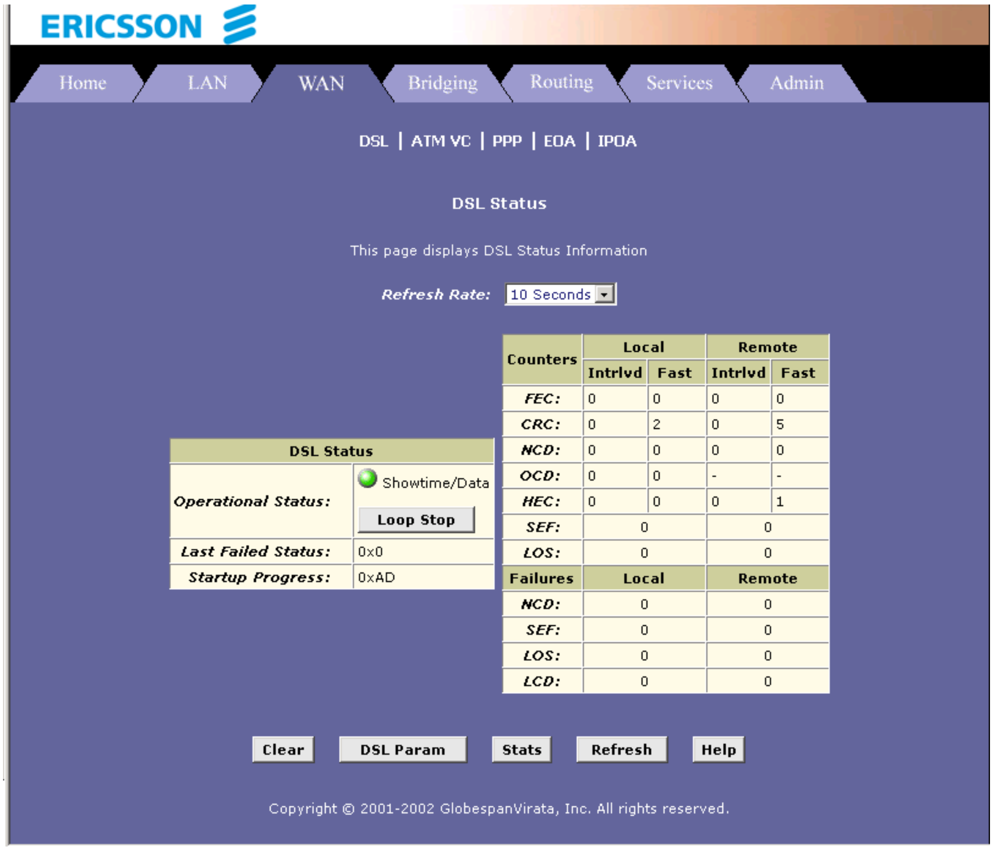
Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Each row in the table displays the time and date when an alarm occurred, the type of alarm and a brief statement indicating its cause.

You can select a recurring time interval in the “*Refresh Rate*” dropdown list after which the page will be redisplayed with new data.

13 Viewing DSL Line Information

To view configuration parameters and performance statistics for the ADSL line, select **WAN > DSL**. The **DSL Status** page displays:



DSL Status

This page displays DSL Status Information

Refresh Rate: 10 Seconds

DSL Status	
Operational Status:	● Showtime/Data Loop Stop
Last Failed Status:	0x0
Startup Progress:	0xAD

Counters	Local		Remote	
	Intrlvd	Fast	Intrlvd	Fast
FEC:	0	0	0	0
CRC:	0	2	0	5
NCD:	0	0	0	0
OCD:	0	0	-	-
HEC:	0	0	0	1
SEF:	0		0	
LOS:	0		0	
Failures	**Local**		**Remote**	
NCD:	0		0	
SEF:	0		0	
LOS:	0		0	
LCD:	0		0	

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

The **DSL Status** page displays the current information on the DSL line performance. The page refreshes about every 10 seconds.

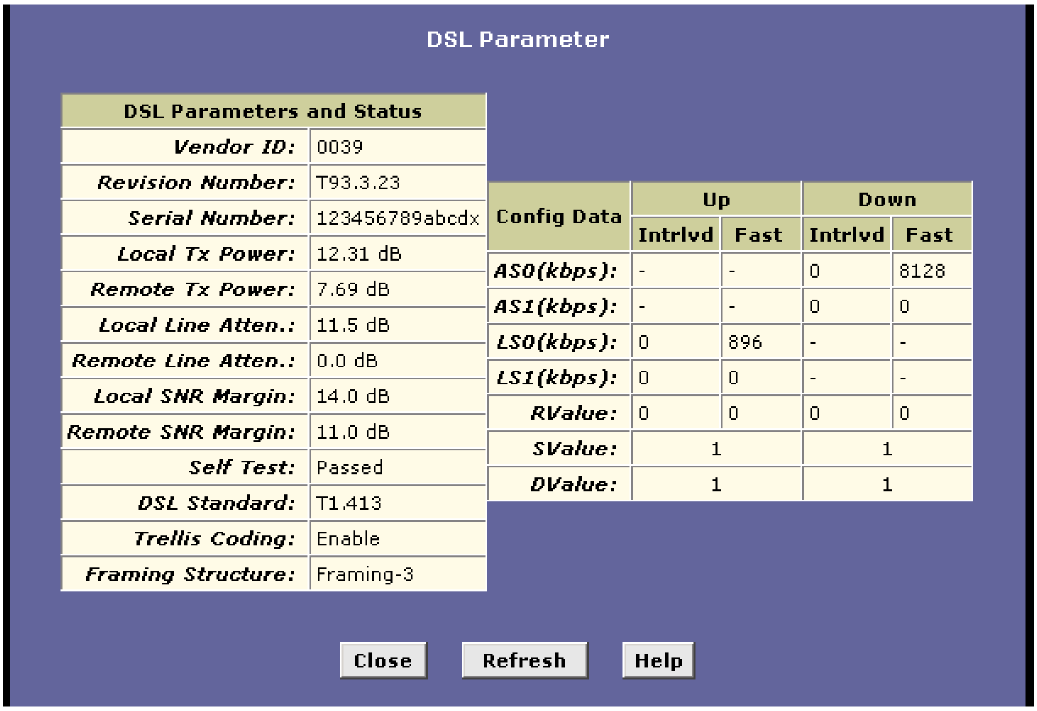
In the DSL Status table, the *Operational Status:* setting displays a red, orange, or green ball to indicate that the DSL line is idle, starting up, or up-and-running, respectively.

You can click the **Loop Stop** to end the DSL connection. To restart the connection, you can click **Loop Start**.

Although you generally will not need to view the remaining data, it may be helpful when troubleshooting connection or performance problems with your ISP.

You can click the **Clear** button to reset all counters to zero, and the **Refresh** button to redisplay the page with newly accumulated values.

You can click the **DSL Param** button to display data about the configuration of the DSL line, as shown below:



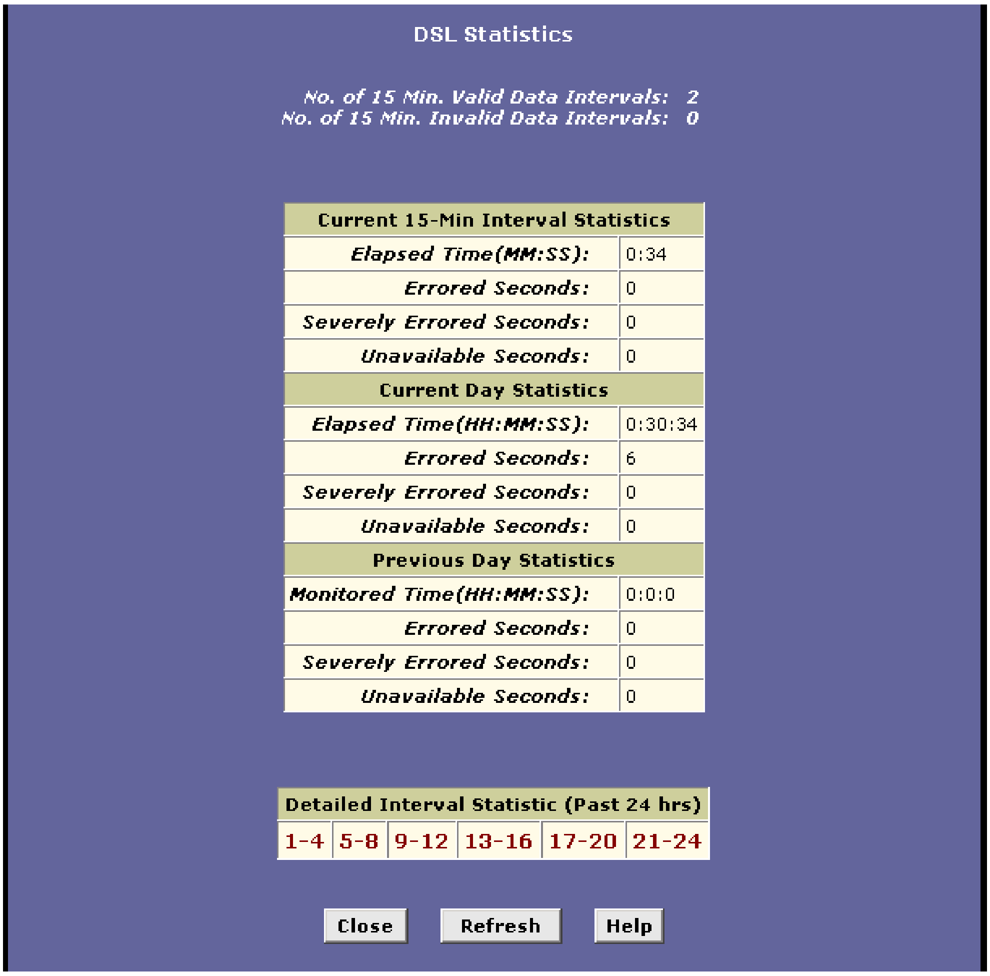
DSL Parameter

DSL Parameters and Status	
Vendor ID:	0039
Revision Number:	T93.3.23
Serial Number:	123456789abcdx
Local Tx Power:	12.31 dB
Remote Tx Power:	7.69 dB
Local Line Atten.:	11.5 dB
Remote Line Atten.:	0.0 dB
Local SNR Margin:	14.0 dB
Remote SNR Margin:	11.0 dB
Self Test:	Passed
DSL Standard:	T1.413
Trellis Coding:	Enable
Framing Structure:	Framing-3

Config Data	Up		Down	
	Intrlvd	Fast	Intrlvd	Fast
AS0(kbps):	-	-	0	8128
AS1(kbps):	-	-	0	0
LS0(kbps):	0	896	-	-
LS1(kbps):	0	0	-	-
RValue:	0	0	0	0
SValue:	1		1	
DValue:	1		1	

The **DSL Parameters and Status** table displays settings preconfigured by the product manufacturer or your ISP.
The **Config Data** table lists various types of error and defects measurements found on the DSL line.
You cannot modify this data.

From the **DSL Status** page you can also click the **Stats** button to display DSL line performance statistics as shown below:



DSL Statistics

No. of 15 Min. Valid Data Intervals: 2
No. of 15 Min. Invalid Data Intervals: 0

Current 15-Min Interval Statistics	
Elapsed Time(MM:SS):	0:34
Errored Seconds:	0
Severely Errored Seconds:	0
Unavailable Seconds:	0
Current Day Statistics	
Elapsed Time(HH:MM:SS):	0:30:34
Errored Seconds:	6
Severely Errored Seconds:	0
Unavailable Seconds:	0
Previous Day Statistics	
Monitored Time(HH:MM:SS):	0:0:0
Errored Seconds:	0
Severely Errored Seconds:	0
Unavailable Seconds:	0

Detailed Interval Statistic (Past 24 hrs)					
1-4	5-8	9-12	13-16	17-20	21-24

The **DSL Statistics** page reports error data relating to the last 15 minutes interval, the current day, and the previous day.

At the bottom of the page, the **Detailed Interval Statistic** table displays links you can click to display detailed data for each 15 minute interval in the past 24 hours. For example, when you click on 1-4, data displays for the 15-minute such intervals that make up the previous 4 hours (there are 16 of these) shows one such page.

14 Troubleshooting

This chapter suggests solutions for resolving some of the problems you might encounter when using your HM210dp/di, and provides instructions for using several IP utilities to diagnose problems.

14.1 LEDs

Indication/Symptom	Troubleshooting Suggestion
The PWR LED does not illuminate after the product is turned on.	Verify that you are using the power cable provided with the device and that it is securely connected to the HM210dp/di and a wall socket/power strip.
The WAN LED does not illuminate after the ADSL cable is attached.	Verify that a standard telephone cable (called an RJ-11 cable) like the one provided is securely connected to the ADSL port and your wall pone jack. Allow about 30 seconds for the device to negotiate with your ISP.
The LAN LED does not illuminate after Ethernet cable is attached.	Verify that the Ethernet cable is securely connected to your LAN hub or PC and to the HM210dp/di. Make sure the PC and/or hub is turned on. Verify that you are using a straight-through type Ethernet cable to the uplink port on a hub or a cross-over type cable to a stand-alone PC. Verify that your cable is sufficient for your network requirements. A 100 Mbit/sec network (10BaseTx) should use cables labeled CAT 5. A 10 Mbit/sec network may tolerate lower quality cables.
The DIAG LED stays illuminated after turning the device on.	The DIAG LED should turn off after about 10-15 seconds. If it does not, turn off the HM210dp/di, wait for 10 seconds, and then turn it back on.

14.2 Internet Access

Indication/Symptom	Troubleshooting Suggestion
My PC cannot access the Internet.	Use the PING utility described below to check whether your PC can communicate with the HM210dp/di's LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling.
	If you statically assigned a private IP address to the computer, verify the following: (Use the WINIPCFG (Windows 98/ME) or IPCONFIG (Windows 2000/XP) utility described below to check your computer(s) have compatible IP addresses) Verify that the DNS server IP address specified on the PCs is correct for your ISP. If you specified that the DNS server be assigned dynamically from a server, then verify with your ISP that the address configured on the HM210dp/di is correct. Then, you can use the PING utility to test connectivity with your ISP's DNS server. Verify with your ISP that the DNS server specified for the PC is valid. Correct the address or configure the PC to receive this information automatically. Verify that a Network Address Translation rule has been defined on the HM210dp/di to translate the private address to your public IP address. The assigned IP address must be within the range specified in the NAT rules. Or, configure the PC to accept an address assigned by another device. The default configuration includes a NAT rule for all dynamically assigned addresses within a predefined pool.
	If you connect using a Username and Password, make sure you have entered them exactly as provided, i.e. distinguish between uppercase and lowercase letters.

14.3 Configuration Manager Program

Indication/Symptom	Troubleshooting Suggestion
I forgot/lost my Configuration Manager Username or Password.	If you have not changed the password from the default, try using **root** as both the Username and Password. Otherwise, you can reset the device to the default configuration by pressing the Reset button on the back panel of the device (using a pointed object such as a pen tip). Then, type the default Username and password as shown above. **WARNING:** Resetting the device removes any custom settings and returns all settings to their default values.
I cannot access the Configuration Manager program from my browser.	Use the PING utility to check whether your PC can communicate with the HM210dp/di's LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling. Verify that you are using Internet Explorer v5.0 or later, or Netscape Navigator v6.1 or later. Support for Javascript® must be enabled in your browser. Support for Java® may also be required. Verify that the PC's IP address is defined as being on the same subnet as the IP address assigned to the LAN port on the HM210dp/di.
My changes to Configuration Manager are not being retained.	Be sure to use the **Commit** function after any changes.

14.4 Diagnosing Problem Using IP Utilities

14.4.1 How to use WINIPCFG

This utility is used mainly to view, release and renew you PCs IP address configuration.

Use WINIPCFG if your PC is running Windows 95, 98 or Me:

1. From the **Start** menu select **Run…** .

2. Type **winipcfg** and click **OK**. The “IP Configuration” dialog box appears.

3. From the scroll down menu at the top, select the network card that you are using. This is important if you have more than one network card.

4. Make sure that the Default gateway is the IP address of your HM210dp/di. If it is not, you will not be able to connect to the Internet.

   If you are using DHCP, click the **Release** and then the **Renew** buttons to receive the correct IP settings.

   If you manually set your network settings, make sure that the IP address of your HM210dp/di is set in the Gateway portion of the TCP/IP settings in your network settings.

5. Click **OK** to close the “IP Configuration” dialog box.

14.4.2 How to use IPCONFIG

This utility is used mainly to view, release and renew you PCs IP address configuration.

Use IPCONFIG if your PC is running Windows NT, 2000 or XP:

1. From the **Start** menu select **Programs > Accessories > Command Prompt**. The “Command Prompt” window appears.

2. Type **ipconfig** to display your IP configuration.

3. Make sure that the Default gateway is the IP address of your HM210dp/di. If it is not, you will not be able to connect to the Internet.

   If you are using DHCP, type **ipconfig /release** and when the C:\> prompt appears again type **ipconfig /renew** to receive the correct IP settings.

4. Close the “Command Prompt” window.

14.4.3 How to use PING

PING is a command you can use to check whether your PC can recognize other computers on your network and the Internet. A ping command sends a message to the computer you specify. If the computer receives the message, it sends messages in reply. To use it, you must know the IP address of the computer with which you are trying to communicate.

You can execute a ping command from the Start menu.

1. From the **Start** menu select **Run…**. The “Run” window appears.

2. Type **ping 192.168.1.1** and click **OK.** You can substitute any private IP address on your LAN or a public IP address for an Internet site, if known.

3. If the target computer receives the messages, a “Command Prompt” window displays with a “Reply” message.

4. If the target computer cannot be located, you will receive the message “Requested timed out”.

15 Important Information

15.1 Product Care and Maintenance

NOTE! These are important guidelines for safe and efficient use of your device. Read this information before using your Ericsson ADSL Modem HM210dp/di.

Your ADSL Modem HM210dp/di is a highly sophisticated electronic device. To get the most out of your product, be sure to read the following text about product care, safety and efficient use.

Do not expose the product to liquid or moisture.

Do not expose the product to extreme temperatures, neither hot nor cold.

Do not expose the product to lit candles, cigarettes, cigars, open flames, etc.

Do not drop, throw or try to bend the product. Rough treatment may damage the product.

Do not attempt to disassemble your product. The warranty is no longer valid if the warranty seal has been broken. The product does not contain consumer serviceable components. Service should only be performed by Certified Service Centers.

Do not allow children to play with the product as it contains small parts that could be detached and create a choking hazard.

Avoid using this telephone equipment during an electrical storm. There may be a remote risk of electric shock from lightning.

Use only original Ericsson components and replacement parts. Failure to do so may result in performance loss, damage to the product, fire, electric shock or injury; and will invalidate the warranty.

Use only the power supply adapter that comes with the unit. Replacement power supply adapters can be obtained from Ericsson upon request.

Treat the product with care, keep it in a clean and dust free place. Use only a soft, damp cloth to clean the product.

15.2 License Agreement

This is a legal agreement, Agreement, between you, Licensee, the recipient of the enclosed Software on compact disc, diskette or any other media and any upgrades thereof, and Ericsson AB, the Vendor. By opening the sealed software package and/or using the software you are agreeing to be bound by the terms of this Agreement.

15.2.1 License

The Licensee is hereby granted a non-transferable, non-exclusive; restricted right and license to use the software included herein, software. However, the Software licensed hereunder may be delivered in an inseparable package also containing other software programs than the Software.

You may: (a) use the enclosed Software on a single Ericsson product; (b) make copies of the Software solely for purposes of backup. The copyright notice must be reproduced and included on a label on any backup copy.

You may not: subject to when applicable, the EC Council Directive of May 14, 1991 on the legal protection of computer programs (91/250/EEG) ("Software Directive" Article 6) distribute copies of this Software or its documentation to others; modify, rent, lease or grant your rights to this Software to third parties (except in the event the Ericsson product containing an item of Software is transferred to a third party and provided the transferee agrees in writing to be bound by the terms of this License Agreement; translate, reverse engineer, decompile, disassemble or otherwise alter the Software or its documentation or disclose any information designated as confidential or proprietary at the time of disclosure or, by nature, is confidential or proprietary.

15.2.2 Term

Your license remains effective from the date of receipt until terminated. You can terminate it at any other time by destroying the Software together with all copies of the Software in any form. Your license will also automatically terminate without notice if you fail to comply with any term or condition of this Agreement. Upon any termination you must destroy all copies of the Software in any form.

15.2.3 Limited Warranty

Vendor warrants the media, on which the Software is provided, to be free of defects in materials and workmanship under normal use for ninety (90) days after the date of receipt. The Vendor's and its suppliers' entire liability and your exclusive remedy under this warranty (which is subject to you returning the Software to an certified reseller with a copy of your receipt) will be, at Vendor's option, to replace the disc(s)/ diskette(s) or refund the purchase price for the Software and terminate this Agreement.

Except for the above express limited warranties, Vendor and its suppliers make and you receive no warranties or conditions either express, implied, statutory or otherwise and Vendor and its suppliers specifically disclaim any implied warranties of merchantability and fitness for a particular purpose. Vendor does not warrant that the Software will be uninterrupted or error free. You assume the responsibility for the selection of the program and hardware to achieve your intended results; and for the installation, use and results obtained from the Software.

Some jurisdictions do now allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

15.2.4 Intended Use

The Software shall be used in accordance with the instructions and for its intended use and purpose only. The software or part of it is not permitted to be used in form example life support systems, nuclear facility applications, missile technology, chemical or biologized industry or of flight navigation or communication of air, ground support equipment or other similar business, if failure to perform on behalf of the software in any way, could result in personal injury, death, damage or tangibles or environmental damage.

15.2.5 Limitation of Liability

If no event shall Vendor or its suppliers be liable for any indirect or consequential losses or damages whatsoever including loss of data, loss of business, loss of profits, business interruption or personal injury arising out of the use of or inability to use this Software. Vendor and its supplier’s entire liability under this Agreement shall be limited to the amount actually paid by Licensee for the Software.

15.2.6 Governing Law

The validity, construction and performance of this Agreement shall be governed by the laws of Sweden.

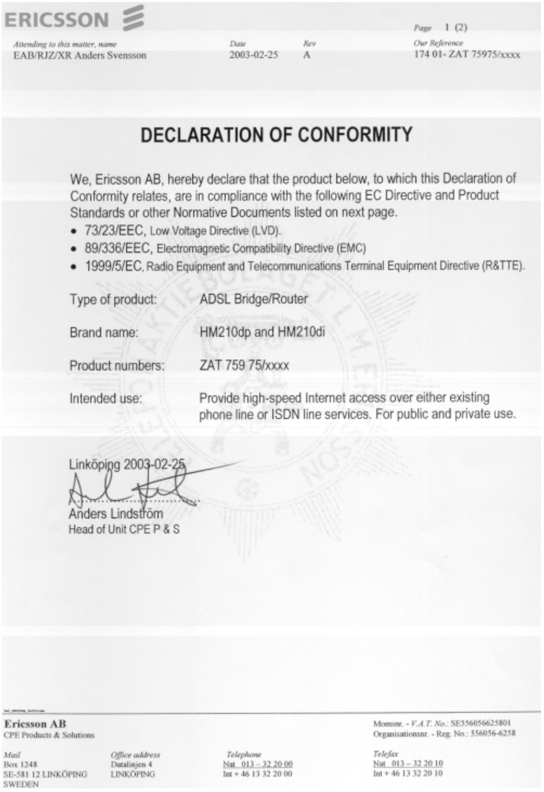
15.3 Regulatory Information

15.3.1 EU Directives

The HM210dp/di meet the following EU directives for the CE-mark:

- 73/23/EEC, Low Voltage Directive (LVD)
- 89/336/EEC, Electromagnetic Compatibility Directive (EMC)
- 1999/5/EC, Radio Equipment and Telecommunication Terminal Directive (R&TTE).

15.3.1.1 Declaration of Conformity



ERICSSON

Page 1 (2)

Attending to this matter, name	Date	Rev	Our Reference
EAB/RJZ/XR Anders Svensson	2003-02-25	A	174 01- ZAT 75975/xxxx

DECLARATION OF CONFORMITY

We, Ericsson AB, hereby declare that the product below, to which this Declaration of Conformity relates, are in compliance with the following EC Directive and Product Standards or other Normative Documents listed on next page.

- 73/23/EEC, Low Voltage Directive (LVD).
- 89/336/EEC, Electromagnetic Compatibility Directive (EMC)
- 1999/5/EC, Radio Equipment and Telecommunications Terminal Equipment Directive (R&TTE).

Type of product: ADSL Bridge/Router

Brand name: HM210dp and HM210di

Product numbers: ZAT 759 75/xxxx

Intended use: Provide high-speed Internet access over either existing phone line or ISDN line services. For public and private use.

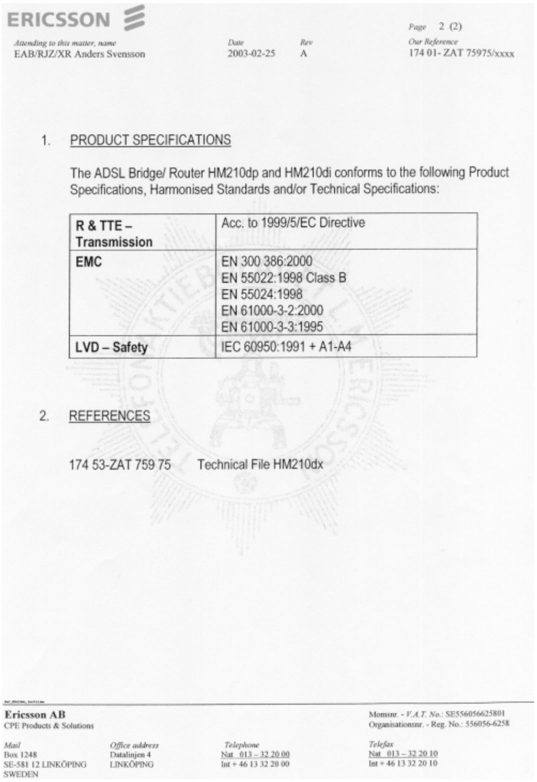
Linköping 2003-02-25

Anders Lindström
Head of Unit CPE P & S

Ericsson AB
CPE Products & Solutions

Momsnr. - V.A.T. No.: SE556056625801
Organisationsnr. - Reg. No.: 556056-6258

Mail	Office address	Telephone	Telefax
Box 1248 SE-581 12 LINKÖPING SWEDEN	Datalinjen 4 LINKÖPING	Nat 013 – 32 20 00 Int + 46 13 32 20 00	Nat 013 – 32 20 10 Int + 46 13 32 20 10



ERICSSON

Page 2 (2)

Attending to this matter, name	Date	Rev	Our Reference
EAB/RJZ/XR Anders Svensson	2003-02-25	A	174 01- ZAT 75975/xxxx

1. PRODUCT SPECIFICATIONS

The ADSL Bridge/ Router HM210dp and HM210di conforms to the following Product Specifications, Harmonised Standards and/or Technical Specifications:

R & TTE – Transmission	Acc. to 1999/5/EC Directive
EMC	EN 300 386:2000 EN 55022:1998 Class B EN 55024:1998 EN 61000-3-2:2000 EN 61000-3-3:1995
LVD – Safety	IEC 60950:1991 + A1-A4

2. REFERENCES

174 53-ZAT 759 75 Technical File HM210dx

Ericsson AB
CPE Products & Solutions

Momsnr. - V.A.T. No.: SE556056625801
Organisationsnr. - Reg. No.: 556056-6258

Mail	Office address	Telephone	Telefax
Box 1248 SE-581 12 LINKÖPING SWEDEN	Datalinjen 4 LINKÖPING	Nat 013 – 32 20 00 Int + 46 13 32 20 00	Nat 013 – 32 20 10 Int + 46 13 32 20 10

15.3.2 Safety Approvals

The HM210dp/di is approved according to the following safety standards:

- UL 1950, 3rd Edition.

- ❑ CSA-C22.2 No. 60950
- ❑ IEC 60950 3rd Edition: 1999

15.3.2.1 UL 1950 Statement

When using your telephone equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

1. Do not use this product near water, for example, near a bathtub, washbowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.
2. Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
3. Do not use the telephone to report a gas leak in the vicinity of the leak.
4. Use only the power cord and batteries indicated in this manual. Do not dispose of batteries in a fire. They may explode. Check with local codes for possible special disposal instructions.

CAUTION! Always disconnect all telephone lines from the wall outlet before servicing or disassembling this equipment.

15.3.3 EMC Approvals

The HM210dp/di is approved according to the following EMC standards:

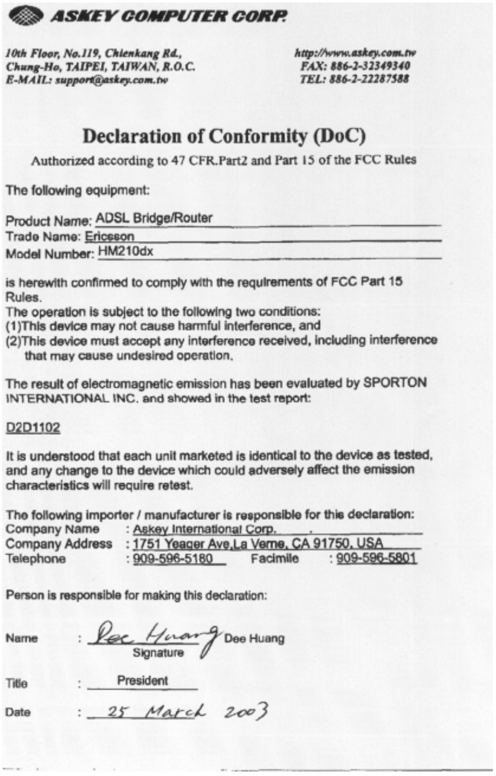
- ❑ EN 300386:2000
- ❑ EN 55022:1998 Class B
- ❑ EN 55024:1998
- ❑ EN 61000-3-2:2000
- ❑ EN 61000-3-3:1995
- ❑ FCC Part 15, Class B, ANSI C63.4-1992

15.3.3.1 FCC Part 15 Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules (Code of Federal Regulations Title 47, Telecommunications (CFR 47)). These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with these instructions, may cause harmful interference to radio or television reception. However, there is no guarantee that interference will occur in particular installation. If this equipment does cause harmful interference to radio or television, which can be determined by turning the equipment off and on, the user is encouraged to eliminate the interference by one or more of the following measures:



ASKEY COMPUTER CORP.

10th Floor, No.119, Chienkang Rd.,
Chung-Ho, TAIPEI, TAIWAN, R.O.C.
E-MAIL: support@askey.com.tw

http://www.askey.com.tw
FAX: 886-2-32349340
TEL: 886-2-22287588

Declaration of Conformity (DoC)

Authorized according to 47 CFR.Part2 and Part 15 of the FCC Rules

The following equipment:

Product Name: ADSL Bridge/Router
Trade Name: Ericsson
Model Number: HM210dx

is herewith confirmed to comply with the requirements of FCC Part 15 Rules.
The operation is subject to the following two conditions:
(1)This device may not cause harmful interference, and
(2)This device must accept any interference received, including interference that may cause undesired operation.

The result of electromagnetic emission has been evaluated by SPORTON INTERNATIONAL INC. and showed in the test report:

D2D1102

It is understood that each unit marketed is identical to the device as tested, and any change to the device which could adversely affect the emission characteristics will require retest.

The following importer / manufacturer is responsible for this declaration:
Company Name : Askey International Corp.
Company Address : 1751 Yeager Ave,La Verne, CA 91750, USA
Telephone : 909-596-5180 Facimile : 909-596-5801

Person is responsible for making this declaration:

Name : Dee Huang Dee Huang
Signature

Title : President

Date : 25 March 2003

- ❑ Reorient or relocate the receiving antenna of the affected equipment.
- ❑ Increase the separation between the ADSL Modem HM210dp/di and the affected equipment.
- ❑ Connect the ADSL Modem HM210dp/di power supply to an outlet on a circuit different from that to which the affected equipment is connected.
- ❑ Consult your service provider or an experienced radio/TV technician for help.

15.3.4 Telecom Approval

The HM210dp/di is approved according to the following telecom standard:

- FCC Part 68

15.3.4.1 FCC Part 68 Statement

The Federal Communications Commission (FCC) has established Rules which permit this device to be directly connected to the telephone network. Standardized jacks are used for these connections. This equipment should not be used on party lines or coin phones.

If this device is malfunctioning, it may also be causing harm to the telephone network; this device should be disconnected until the source of the problem can be determined and until repair has been made. If this is not done, the telephone company may temporarily disconnect service.

The telephone company may make changes in its technical operations and procedures; if such changes affect the compatibility or use of this device, the telephone company is required to give adequate notice of the changes. You will be advised of your right to file a complaint with the FCC.

If the telephone company requests information on what equipment is connected to their lines, inform them of:

- The telephone number to which this unit is connected
- The USOC jack required
- The FCC Registration Number (indicated on the label).

The Ringer Equivalence Number (REN). Note that if several devices are connected on the same line, the RENs must not add up to more than 5.0. This REN figure is important to your telco and can be found on the equipment's FCC compliance label.

In case of operational problems, disconnect your unit by removing the modular or multi-connector plug from the telco's jack. If your regular phone still works properly, your modem has a problem and must remain disconnected and (officially) serviced or returned for repairs. If upon the above disconnection your regular phone still has problems, notify your telco that they may have a problem. If problem is still found in premises wiring not telco-installed, you are subject to a service charge. If a fault is found in telco-installed wiring, you may still be subject to a service call charge.

Unless otherwise noted in the User's Manual (e.g. fuses, etc), user may not under any circumstances (in or out of warranty) attempt any service adjustment, or repairs on this unit. It must be returned to the factory or authorized U.S. service agency for all such work. Locations and phone number of factory or authorized U.S. service points are as following:

Special FCC rules apply to equipment connected behind a PBX or KTS.

Company: Ericsson Inc.
Address: 6300 Legacy Drive, Plano, TX 75024, USA
Tel: 972-583-2000.

15.3.5 Caution

Changes or modifications to this product not authorized by the manufacturer could void your authority to operate the equipment and invalidate approvals.

15.3.6 Power Supply

The ADSL Modem HM210dp/di is equipped with one of the following external power supply adapters:

- **For EU**
  OEM type: AA-161ABN. Input: 230 VAC, 50Hz. Output: 16VAC, 1A
  or
  OEM type: AA-1860BN. Input: 230 VAC, 50Hz. Output: 18VAC, 600mA

- **For US**
  OEM type: AA-161A. Input: 120VAC, 60Hz. Output: 16VAC, 1A
  or
  OEM type: AA-1860. Input: 120 VAC, 60Hz. Output: 16VAC, 600mA.

NOTE! The ADSL Modem HM210dp/di is for use only with one of the above approved power supply adapter. In the event of equipment malfunction, replace only with an AC/DC Adapter specified by Ericsson.

15.3.7 Environmental Information

Maximum environmental values during use:

- Temperature: 0^{o}C to $+45^{o}$C

- Humidity: 5% to 95% RH, non-condensing.

15.3.8 Intended Use

The HM210dp/di is intended for indoor public and private use.

16 Glossary

- A -

ADSL
Short for ***A**symmetric **D**igital **S**ubscriber **L**ine*. A variation of the DSL technologies that is most familiar to home and small business users. ADSL is called "asymmetric" because most of its two-way or duplex bandwidth is devoted to the downstream direction, sending data to the user. Only a small portion of bandwidth is available for upstream or user-interaction messages.

ARP
Short for ***A**ddress **R**esolution **P**rotocol*, a TCP/IP protocol used to convert an IP address into a physical address, such as an Ethernet address. A host wishing to obtain a physical address broadcasts an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address.
There is also Reverse ARP (RARP) which can be used by a host to discover its IP address. In this case, the host broadcasts its physical address and a RARP server replies with the host's IP address.

ATM
Short for ***A**synchronous **T**ransfer **M**ode*, a network technology based on transferring data in cells or packets of a fixed size. The cell used with ATM is relatively small compared to units used with older technologies. The small, constant cell size allows ATM equipment to transmit video, audio, and computer data over the same network, and assure that no single type of data hogs the line.

Authenticate
To verify a user's identity, such as by prompting for a password.

- B -

Bridging
Passing data from your network to your ISP and vice versa using the hardware addresses of the devices at each location. Bridging contrasts with routing, which can add more intelligence to data transfers by using network addresses instead. The HM210dp/di can perform both routing and bridging. Typically, when both functions are enabled, the device routes IP data and bridges all other types of data. See also *Routing.*

Broadband
A telecommunications technology that can send different types of data over the same medium. DSL is a broadband technology.

Broadcast
To simultaneously send the same message to multiple recipients.

- C -

CHAP
Short for ***C****hallenge* ***H****andshake* ***A****uthentication* ***P****rotocol*. A type of authentication in which the authentication agent (typically a network server) sends the client program a random value that is used only once and an ID value. Both the sender and peer share a predefined secret.

- D -

Device
Any machine or component that attaches to a computer. Examples of devices include disk drives, printers, mice and modems.

DHCP
Short for ***D****ynamic* ***H****ost* ***C****onfiguration* ***P****rotocol*, which is a protocol for assigning dynamic IP addresses to devices in a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. Many ISPs use dynamic IP addressing for dial-up users.

DHCP Relay
A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses.

DHCP Server
A DHCP server is a computer that is responsible for assigning IP addresses to the computers on a LAN. See also *DHCP.*

DMZ
A ***De****militarized* ***Z****one* is used by a company that wants to host its own Internet services without sacrificing unauthorized access to its private network. The DMZ sits between the Internet and an internal network's line of defense, usually some combination of firewalls and bastion hosts.

DNS
Short for ***D****omain* ***N****ame* ***S****ystem (or* ***S****ervice)*, an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address.

The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Domain name
A domain name is a user-friendly name used in place of its associated IP address

Downstream
The direction of a downstream signal is from the ISP/service provider to the user's computer (downloading).

DSL
Short for ***D**igital* ***S**ubscriber* ***L**ine*, which is a data communications technology that transmits information over the existing copper telephone lines (POTS). DSL takes existing voice cables that connect customer premises (CPE) to the phone company's central office (CO) and turns them into a high-speed digital link. There are many types of DSL and ADSL is one of them.

- E -

Encapsulation
A technology that enables one network to send its data via another network's connections. Encapsulation works by encapsulating a network protocol within packets carried by the second network. Encapsulation is also called tunneling.

Ethernet
A local-area network (LAN) architecture that uses a bus topology and supports data transfer rates of 10 Mbps. It is one of the most widely implemented LAN standards.
A newer version of Ethernet, called 100Base-T (or Fast Ethernet), supports data transfer rates of 100 Mbps. And the newest version, Gigabit Ethernet, supports data rates of 1 gigabit (1,000 megabits) per second.

- F -

Filtering
To screen out selected types of data, based on filtering rules. Filtering can be applied in one direction (upstream or downstream) or in both directions.

Filtering rule
A rule that specifies what kinds of data a routing device will accept and/or reject. Filtering rules are defined to operate on an interface (or multiple interfaces) and in a particular direction (upstream, downstream or both).

Firewall
A system designed to prevent unauthorized access to or from a private

network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security critera.

Firmware
Firmware is a combination of software and hardware consisting of software (programs or data) that has been written onto read-only memory.

FTP
Short for ***F****ile* ***T****ransfer* ***P****rotocol*. A program used to transfer files between computers connected to the Internet. Common uses include uploading new or updated files to a web server, and downloading files from a web server.

- G -

Gateway
A node on a network that serves as an entrance to another network. In enterprises, the gateway is the computer that routes the traffic from a workstation to the outside network that is serving the Web pages. In homes, the gateway is the ISP that connects the user to the Internet.

G.dmt
A kind of asymmetric DSL technology, based on DMT modulation, that offers up to 8 megabits per second downstream bandwidth, 1.544 Megabits per second upstream bandwidth. "G.dmt" is actually a nickname for the standard officially known as ITU-T Recommendation G.992.1.

G.lite
A kind of asymmetric DSL technology, based on DMT modulation, that offers up to 1.5 megabits per second downstream bandwidth, 384 Kilobits per second upstream, does not usually require a splitter and is easier to install than other types of DSL. "G.lite" is a nickname for the standard officially known as G.992.2.

- H -

Hop
When you send data through the Internet, it is sent first from your computer to a router, and then from one router to another until it finally reaches a router that is directly connected to the recipient. Each individual “leg” of the data’s journey is called a hop.

Hop count
The number of hops that data has taken on its route to its destination.

Alternatively, the maximum number of hops that a packet is allowed to take before being discarded (see also *TTL)*.

Host
A computer that is connected to a TCP/IP network, including the Internet. Each host has a unique IP address.

HTTP
Short for ***H**yper**T**ext **T**ransfer **P**rotocol*. HTTP is the main protocol used to transfer data from web sites so that it can be displayed by web browsers.

- I -

ICMP
Short for ***I**nternet **C**ontrol **M**essage **P**rotocol*. An Internet protocol used to report errors and other network related information. The PING command makes use of ICMP.

IGMP
Short for ***I**nternet **G**roup **M**anagement **P**rotocol*. An Internet protocol that enables a computer to share information about its membership in multicast groups with adjacent routers. A multicast group of computers is one whose members have designated as interested in receiving specific content from the others. Multicasting to an IGMP group can be used to simultaneously update the address books of a group of mobile computer users or to send company newsletters to a distribution list.

Internet
The global collection of interconnected networks used for both private and business communications.

Intranet
A private, company-internal network that looks like part of the Internet (users access information using web browsers), but is accessible only by employees.

IP address
An identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255, for example 192.168.0.1.

Public IP addresses are LAN IP addresses that can be considered "legal" for the Internet because they can be recognized and accessed by any device on the other side of a connection. In most cases your ISP allocates them.

Private IP addresses are also LAN IP addresses, but are considered "illegal" IP addresses to the Internet. They are private to an enterprise while still permitting full network layer connectivity between all hosts inside an enterprise as well as all public hosts of different enterprises.

ISP
Short for ***I**nternet **S**ervice **P**rovider*, a company that provides access to the Internet.

- L -

LAN
Short for ***L**ocal **A**rea **N**etwork*, which is a computer network limited to the immediate area, usually the same building or floor of a building. A WAN, on the other hand, is an outside connection to another network or the Internet.

LED
Abbreviation of ***L**ight **E**mitting **D**iode*, a type of control lamp on devices that indicates the status of a device.

- M -

MAC address
Short for ***M**edia **A**ccess **C**ontrol address*. The permanent hardware address of a device, assigned by its manufacturer. MAC addresses are expressed as six pairs of characters.

- N -

NAT
Short for ***N**etwork **A**ddress **T**ranslation*. A service performed by many routers that translate your network's publicly known IP address into a *private **IP*** address for each computer on your LAN. Only your router and your LAN know these addresses; the outside world sees only the public IP address when talking to a computer on your LAN.

NAT rule
A defined method for translating between public and private IP addresses on your LAN.

NIC
Short for ***N**etwork **I**nterface **C**ard*, which is an expansion board you insert into a computer so the computer can be connected to a network. Most NICs are designed for a particular type of network, protocol, and media, although some can serve multiple networks.

- P -

Packet
Data transmitted on a network consists of units called packets. Each packet contains a payload (the data), plus overhead information such as where it came from (source address) and where it should go (destination address).

PAP
Short for ***P**assword **A**uthentication **P**rotocol*, the most basic form of authentication, in which a user's name and password are transmitted over a network and compared to a table of name-password pairs. Typically, the passwords stored in the table are encrypted.

PING
Short for ***P**acket **I**nternet (or **I**nter-**N**etwork) **G**roper*. A program used to verify whether the host associated with an IP address is online. It can also be used to reveal the IP address for a given domain name.

Port
In TCP/IP and UDP networks, an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.

POTS
Short for ***P**lain **O**ld **T**elephone **S**ervice*, which refers to the standard telephone service that most homes use. The POTS network is also called the Public Switched Telephone Network (PSTN).

PPP
Short for ***P**oint-to-**P**oint **P**rotocol*. A protocol for serial data transmission that is used to carry IP (and other protocol) data between your ISP and your computer.

PPPoE
Acronym for ***P**oint-to-**P**oint **P**rotocol **o**ver **E**thernet*. PPPoE relies on two widely accepted standards: PPP and Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet share a common connection, so the Ethernet principles supporting multiple users in a LAN combine with the principles of PPP, which apply to serial connections.

Protocol
A set of rules governing the transmission of data. In order for a data transmission to work, both ends of the connection have to follow the rules of the protocol.

PVC
Short for ***P**ermanent **V**irtual **C**ircuit*, which is a logical point-to-point circuit between customer sites. PVCs are low-delay circuits because routing decisions do not need to be made along the way. Permanent means that

the circuit is preprogrammed by the carrier as a path through the network. It does not need to be set up or disconnected for each session.

- R -

Remote
In a physically separate location. For example, an employee away on travel who logs in to the company's intranet is a remote user.

RFC
Short for ***R**equest **F**or **C**omments*, a series of notes about the Internet, started in 1969 (when the Internet was the ARPANET). An Internet Document can be submitted to the IETF by anyone, but the IETF decides if the document becomes an RFC. Eventually, if it gains enough interest, it may evolve into an Internet standard. Each RFC is designated by an RFC number. Once published, an RFC never changes. Modifications to an original RFC are assigned a new RFC number.

RIP
Short for ***R**outing **I**nformation **P**rotocol*, which is a protocol that specifies how routers exchange routing table information. With RIP, routers periodically exchange entire tables. There are two versions of RIP; version 1 and version II.

Routing
Forwarding data between your network and the Internet on the most efficient route, based on the data's destination IP address and current network conditions. A device that performs routing is called a router.

- S -

SDNS
Short for ***S**econdary **D**omain **N**ame **S**ystem (Server).* A DNS server that can be used if the primary DNS server is not available. See also *DNS.*

SNMP
Short for ***S**imple **N**etwork **M**anagement **P**rotocol,* a set of protocols for managing complex networks. SNMP works by sending messages, called *protocol data units (PDUs)*, to different parts of a network. SNMP-compliant devices, called *agents,* store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

Subnet
A subnet is a portion of a network. The subnet is distinguished from the larger network by a *subnet mask* which selects some of the computers of the network and excludes all others. The subnet's computers remain physically connected to the rest of the parent network, but they are treated as though they were on a separate network.

- T -

T1.413

The American National Standards Institute (ANSI) standard for asymmetric digital subscriber line using discrete multitone modulation, which the G.dmt standard is based on.

TCP

Abbreviation of ***T**ransmission **C**ontrol **P**rotocol*, and pronounced as separate letters. TCP is one of the main protocols in TCP/IP networks. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

TCP/IP

Short for ***T**ransmission **C**ontrol **P**rotocol / **I**nternet **P**rotocol*, the suite of communication protocols used to connect hosts on the Internet.

Telnet

A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console.

TFTP

Short for ***T**rivial **F**ile **T**ransfer **P**rotocol.* A protocol for file transfers. TFTP is easier to use than the File Transfer Protocol (FTP) but is not as capable or secure.

TTL

Short for ***T**ime **T**o **L**ive*. A field in an IP packet that limits the life span of that packet. Originally meant as a time duration, the TTL is usually represented instead as a maximum hop count; each router that receives a packets decrements this field by one. When the TTL reaches zero, the packet is discarded.

- U -

UDP

Short for ***U**ser **D**atagram **P**rotocol*, which is a connectionless transport service that dispenses with the reliability services provided by TCP. UDP gives applications a direct interface with IP and the ability to address a particular application process running on a host via a port number, without setting up a connection session.

Upstream

The direction of an upstream signal is from the user's computer to the ISP/service provider (uploading).

- V -

VC

A VC (***V**irtual **C**ircuit*) is a connection from your ADSL router to your ISP.

VPI and VCI

A VPI (***V**irtual **P**ath **I**dentifier*) is an 8-bit field while VCI (***V**irtual **C**hannel **I**dentifier*) is a 16-bit field in the ATM cell header. A VPI identifies a link formed by a virtual path and a VCI identifies a channel within a virtual path. In this way, the cells belonging to the same connection can be distinguished. A unique and separate VPI/VCI identifier is assigned in advance to indicate which type of cells follow; unassigned cells, physical layer OAM cells, metasignalling channel or a generic broadcast signaling channel. Your ISP should supply you with the values.

- W -

WAN

Short for ***W**ide **A**rea **N**etwork*. A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more Local Area Networks (LANs). Computers connected to a WAN are often connected through public networks, such as the telephone system.